ISTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

SECURITY RISK ASSESSMENT FOR CRITICAL FACILITY PROTECTION

Ph.D. Thesis by
İlker AKGÜN

Department : Industrial Engineering

Programme : Industrial Engineering

JANUARY 2012

ISTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

SECURITY RISK ASSESSMENT FOR CRITICAL FACILITY PROTECTION

Ph.D. Thesis by
İlker AKGÜN
(507042107)

Date of submission : 10 October 2011
Date of defence examination: 03 January 2012

Supervisor (Chairman) : Prof. Dr. Ahmet Fahri ÖZOK (ITU)
Members of the Examining Committee : Prof. Dr. Cengiz KAHRAMAN (ITU)
Prof. Dr. Yasemin C. ERENSAL(DU)
Prof. Dr. Seçkin POLAT (ITU)
Prof. Dr. Coşkun ÖZKAN (KU)

JANUARY 2012

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

KRİTİK TESİSLERİN KORUNMASI İÇİN GÜVENLİK RİSKİ DEĞERLEMESİ

DOKTORA TEZİ

İlker AKGÜN
(507042107)

Tezin Enstitüye Verildiği Tarih : 10 Ekim 2011
Tezin Savunulduğu Tarih : 03 Ocak 2012

Tez Danışmanı : Prof. Dr. Ahmet Fahri ÖZOK (İTÜ)
Diğer Jüri Üyeleri : Prof. Dr. Cengiz KAHRAMAN (İTÜ)
Prof. Dr. Yasemin C. ERENSAL (DÜ)
Prof. Dr. Seçkin POLAT (İTÜ)
Prof. Dr. Coşkun ÖZKAN (KÜ)

OCAK 2012

FOREWORD

I would like to express my sincere gratitude to my leading supervisor, Prof. Dr. Ahmet Fahri ÖZOK. Without his and the surveyor committee members: Prof. Dr. Yasemin Claire ERENSAL and Prof. Dr. Cengiz KAHRAMAN's advise and support this thesis would never had become a reality. Finally, I wish to express my greatest thanks to my family, friends and colleagues, who have supported me, especially to my wife Ahu, for her patience and understanding.

The data used within this thesis are for illustrative purpose only and do not constitute any datasets of any organizations due to the sensitivity of the topic. The views expressed are purely those of the author and may not in any circumstances be regarded as stating an official position of the any organization.

January 2012

İlker AKGÜN, MSc.

Engineer

TABLE OF CONTENTS

Page

ABBREVIATIONS

AL : Asset Loss
ATMS : Air Traffic Management Service
Bel : Belief
bpa : Basic Probability Assignment
CA : Consequence Assessment
CAM : Consequence Assessment Model
CBS : Cargo and Baggage Service
CCA : Cross Consistency Assessment
DM : Decision Maker
DST : Dempster-Shafer Theory of Evidence
EMA : Evidence based Morphological Analysis
ES : Emergency Service
FCM : Fuzzy Cognitive Maps
FD : Frame of Discernment
FIVAM : Fuzzy Integrated Vulnerability Assessment Model
FRA : Fuzzy Risk Assessment
GDM : Group Decision Making
GHS : Ground Handling Service
HL : Human Loss
Ha : Hectare
L : Turkish Lira
Kg : Kilograms
MA : Morphological Analysis
MAUT : Multi Attribute Utility Theory
MCDM : Multiple Criteria/Attribute Decision Making
MPa : Mega Pascal
IS : Infrastructure Service
OL : Operational Loss
PS : Passenger Service
Pls : Plausibility
PRA : Probabilistic Risk Assessment
RA : Risk Assessment
REM : Risk Evaluation Model
SAW : Simple Additive Weight Method
SRA : Security Risk Assessment
SMART : Simple Multi-Attribute Rating Techniques
SWOT : Strength, Weakness, Opportunity and Threat Analysis
TAM : Threat Assessment Model
TFN : Triangular Fuzzy Numbers
TNT : Trinitrotoluene
ULWA : Uncertain Linguistic Weighted Average
VAM : Vulnerability Assessment Model

LIST OF TABLES

Page

LIST OF FIGURES

Page

SECURITY RISK ASSESSMENT FOR CRITICAL FACILITY PROTECTION

SUMMARY

Although many countries have national security challenges, security risk has infiltrated into the international arena just after the attacks to twin towers in New York/USA on September 11, 2001 called 9/11 attacks. The 9/11 attacks are the beginning of the new era where the classical approaches to contemporary security challenges are questioned by security analysts and academics. There is also an increase in malevolent attacks in recent years worldwide. Developed societies become more vulnerable to security risks caused by such events as they get more dependent on critical facilities such as airports, nuclear power plants, oil plants, dams, harbours, governmental facilities etc.

This thesis proposes a novel Security Risk Assessment (SRA) framework consisting of four models that quantifies corresponding security risk factors: threat, vulnerability and consequence, and aggregates them. Proposed SRA framework helps to improve security risk assessment decisions for critical facilities considering appropriate uncertainty theory, input data and output data for each model. The four developed models are presented step-by-step and applied to an illustrative airport as a critical facility case study. Therefore, all the application in each chapter covers an illustrative airport. The results of the applications are evaluated to illustrate the effectiveness of proposed SRA framework.

The thesis consists of six chapters. The first chapter, Introduction introduces the motivation of the study and its aim and objectives. Introductory chapter summarizes also the theoretical, methodological and information processing frameworks utilized in the thesis. Respectively, Chapters 2, 3 and 4 provide threat, vulnerability and consequence assessment models. Then, Chapter 5 provides a model that aggregates the outputs of the threat, vulnerability and consequence assessment models presented until this chapter under a Security Risk Assessment framework. Finally, the study concludes by highlighting the major concluding remarks and offering some recommendations.

Chapter 2 offers a Threat Assessment Model. The aim in this chapter is to identify threats of a critical facility and estimates their likelihoods in order to generate the initiating events, possible threat scenarios, for other models of SRA framework.

The model offered in Chapter 3, Vulnerability Assessment Model identifies and quantifies the weakness of the critical facility as a system, system functions and system components, and determines the most critical functions and components by simulating the system behaviour.

Chapter 4 aims to quantify the likely loss or damage caused due to anticipated threat scenarios. Therefore, the Consequence Assessment Model estimates the expected

magnitude and type of loss (e.g., deaths, injuries, or property damage) associated with a threat scenario given adversary success for a critical facility.

Chapter 5 gathers all the information together and continues the calculation and evaluation in order to aggregate the outputs of Threat Assessment Model, Vulnerability Assessment Model and Consequence Assessment Model for evaluating the security risk of a critical facility. What is offered in Chapter 5 is basically the last step of the SRA framework.

To summarize, this thesis proposes a complete SRA framework that offers a comprehensive and logical multi methodological approach capable of handling and combining different uncertainties for assessing the security risk of critical facilities. Illustrative case study shows that useful insight about possible security risks of a critical facility can be gained through applying proposed SRA framework and proposed framework provides valuable information to decision makers in dealing with security risks of critical facility by increasing situational awareness and understanding. As a result, proposed SRA framework has contributed to quantitative decision analysis by supporting decisions under different modes of uncertainty and provided a basis for more effective security risk management.

KRİTİK TESİSLERİN KORUNMASI İÇİN GÜVENLİK RİSKİ DEĞERLEMESİ

ÖZET

Pek çok ülkede ulusal güvenlik sorunları olmasına rağmen, 11 Eylül 2001 tarihinde New York / ABD ikiz kuleler saldırılarından - 9 / 11 saldırıları - hemen sonra güvenlik riski uluslararası arenanın gündemine girmiştir. 9/11 saldırıları, güvenlik analizcileri ve akademisyenler tarafından güncel güvenlik konularına klasik yaklaşımların sorgulandığı yeni bir çağın başlangıcı olmuştur. Ayrıca, son yıllarda dünya çapında kötü niyetli saldırılar daha da artmaktadır. Gelişmiş toplumlar, havaalanı, nükleer enerji santrali, petrol istasyonu, barajlar, limanlar, kamu tesisleri gibi kritik tesislere git gide daha bağımlı hale geldikleri için bu tür kötü niyetli saldırılara karşı daha savunmasız hale gelmektedir.

Bu tez güvenlik riski faktörleri olan tehdit olabilirliğini, güvenlik açığını ve oluşabilecek hasarı sayısallaştıracak ve birleştirecek dört modeli içeren yeni bir Güvenlik Riski Değerlemesi (GRD) çerçevesi önermektedir. Önerilen GRD çerçevesi, belirsizlik kuramı, girdi verisi ve çıktı verisini her model için dikkate alarak kritik tesisler için GRD kararlarını geliştirmede yardımcı olmaktadır. Geliştiren dört model adım adım sunulmakta ve kritik tesisler için örnek uygulama olarak havalimanına uygulanmaktadır. Böylece, her bir bölümde ayrı ayrı verilen tüm uygulamalarda havalimanı örneği kullanılmaktadır. Uygulamaların sonuçları önerilen GRD çerçevesinin etkinliğini göstermek için değerlendirilmektedir.

Tez altı bölümden oluşmaktadır. İlk bölüm olan, giriş bölümü çalışmanın çıkış noktasını, amacını ve hedeflerini tanıtmaktadır. Giriş bölümü ayrıca tez de kullanılan kuramsal, yöntemsel ve bilgi işleme çerçevelerini de özetlemektedir. Sırasıyla, Bölüm 2,3 ve 4 tehdit, güvenlik açığı ve hasar değerleme modellerini ortaya koymaktadır. Sonrasında, Bölüm 5 bu modellerin çıktılarını Güvenlik Riski Değerlemesi çerçevesi adı altında tek bir modelde bütünleştirmektedir. Son olarak, çalışma temel sonuç değerlendirmelerini vurgulayarak ve bazı önerilerde bulanarak sonuçlanmaktadır.

Bölüm 2, Tehdit Değerleme Modelini sunmaktadır. Bu bölümde amaç, başlangıç olayları olan olası tehdit senaryolarını diğer GRD çerçevesindeki modeller için üreterek kritik tesislerin karşı karşıya kaldığı tehditleri belirlemek ve olabilirliklerini tahmin etmektir.

Bölüm 3'te sunulan model, Güvenlik Açığı Değerleme Modeli ise kritik tesisleri sistem yaklaşımı çerçevesinde bir sistem, sistem işlevleri ve sistem bileşenleri olarak ele almakta ve bu tesislerin zayıflıklarını belirlemekte ve sayısallaştırmakta, ayrıca en kritik işlevi ve bileşeni sistemin davranışlarının benzetimini yaparak saptamaktadır.

Bölüm 4, beklenen tehdit senaryolarınca meydana gelebilecek muhtemel kayıpları veya hasarları sayısallaştırmayı amaçlamaktadır. Böylece, Hasar Değerleme Modeli kritik tesis için saldırganın başarı sağlayabileceği bir tehdit senaryosunda beklenen kayıp büyüklüğünü ve kayıp türünü (ölüm, yaralanma veya makine/teçhizat kaybı vs.) tahmin etmektedir.

Bölüm 5 tüm model çıktılarını bir araya getirip Tehdit Değerleme Modelinin, Güvenlik Açığı Değerleme Modelinin ve Hasar Değerleme Modelinin çıktılarını bütünleştirerek kritik tesis için güvenlik riski değerlendirmesi yapmaktadır. Bu bölümdeki model GRD çerçevesi içi son adımdır.

Özet olarak, bu çalışma bütüncül bir GRD çerçevesi ve kritik tesisler için güvenlik riski değerlemede farklı belirsizlikleri ele alabilen ve bu belirsizlikleri birleştirebilir bütünsel ve mantıksal çoklu yöntem yaklaşımı sunmaktadır. Örnek uygulama göstermektedir ki, önerilen GRD çerçevesi uygulanarak kritik tesislerin olası güvenlik riskleri hakkında kullanışlı sezgiler kazanılmakta ve önerilen çerçeve durumsal farkındalığı ve anlamayı arttırarak kritik tesislerin güvenlik riski ile başa çıkmada karar vericilere değerli bilgiler sunmaktadır. Sonuç olarak, önerilen GRD çerçevesi, farklı belirsizlikler içinde alınan kararları destekleyerek sayısal karar analizine katkıda bulunmakta ve daha etkin bir güvenlik riski yönetimine zemin sağlamaktadır.

1. INTRODUCTION

Although many countries have national security challenges, security risk has infiltrated into the international arena just after the attacks to twin towers in New York/USA on September 11, 2001 called 9/11 attacks. The 9/11 attacks are the beginning of the new era where the classical approaches to contemporary security challenges are questioned by security analysts and academics (Harris, 2004; Wright et al., 2006; Keeney, 2007). The notion of the change in security mainly stems from the changes in targets, weapons, and motives, the combination of which make malevolent attacks more dangerous than ever before. There is also an increase in malevolent attacks in recent years worldwide. Weapons such as explosives meanwhile became more lethal and efficient, and the technology and skills enabled them diffuse throughout the world easily. As a result of these progresses, developed societies become more vulnerable to security risks as they more get more dependent on critical facilities. In developed societies, critical facilities are the systems that have a high impact to the psychology, health and welfare of the population, and are essential to the operations of the economy and government such as airports, nuclear power plants, oil plants, dams, harbours, governmental facilities etc. Therefore, critical facilities are attractive targets for malevolent attacks and should be given special consideration for security risk assessment (SRA). Traditionally, studies on security have focused on military and defence issues but security in military terms is inadequate at present. During this change of the profile of security, 9/11 attacks displayed that even the most powerful can not be immune to such attacks and reminded that there is an obvious need to revisit security risk with a view to proposing adequate responses to emerging threats rather than military threats.

1.1 Background – Motivation of the Study

Risk traditionally has a negative meaning and can be defined both qualitatively and quantitatively. According to the qualitative definition of risk, which is the dictionary definition, risk is “exposure to the possibility of loss, injury, or other adverse or

unwelcome circumstance; a chance or situation involving such a possibility" (Simpson and Weiner, 1989). The quantitative definition of risk is commonly defined as a measure of expected loss which is the product of likelihood and severity of loss based on the probability theory in the literature.

To manage risk in an efficient way, risk assessment (RA) is required. RA is a systematic decision analysis methodology for identifying the expected loss incurred by a system or process as a result of undesired event. Typical RA is generally related to expected losses from failures, accidents, and natural disasters and is a kind of safety analysis. There are different sources of risk and Renn (1992) identifies five major types of RA: technical RA, economic RA, psychological RA, sociological RA and cultural RA. The first two types of RA are quantitative and the last three are qualitative. Each of RA has different assumptions about the underlying reality under consideration depending on the concerned risk type. For example, in economic RA, risk is associated with the unexpected variability or volatility of returns.

However, risk of random events is different from risk of intelligent events. The risk arising from intelligent acts is called security risk. Security risk includes intelligent, deliberate, and unpredictable acts which are intended to create fear, are committed for an ideological goal, and deliberately target or disregard the safety of civilians (Garrick et al., 2004). Security risk differs in kind from other type of risks because of these special characteristics. Thus, protecting against security risk is fundamentally different from protecting against natural disasters or accidents and has to be handled in a different way. In the literature, most researchers agree that security risk is based on the analysis and aggregation of three widely recognized factors: threat likelihood, vulnerability, and consequence as (Willis et al., 2005):

$$\text{Security Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence} \quad \textbf{(1.1)}$$

Threat is the likelihood of the malevolent attack, vulnerability is the system response to attack and the consequence is the result of the attack. Each security risk has a corresponding likelihood, vulnerability and consequence. Security analysts attempt to answer following three fundamental questions related to these factors: "How likely is it?", "What can go wrong?", and "How bad it can be?" (Kaplan and Garrick, 1981). In the security domain, RA focuses on assessing the likelihood of attack, likelihood of adversary success given attack, and consequences given success for a

variety of threat scenarios. Equation 1.1 provides the main basis for many SRA methodologies (Garrick et al., 2004). As in the other typical risk types, to manage security risk in an efficient way, SRA is required. Managing security risk through threat likelihood requires intelligence represent an approach to SRA that focuses specifically on threats. Managing security risk through vulnerability requires increasing surveillance and detection, hardening targets, or other capabilities that might reduce the success of attempted attacks. Managing security risk through consequences can be done through increasing preparedness and response that reduces the effects of damage through mitigation or compensation. The main problems are how these factors are quantified and aggregated.

Therefore, SRA is an important and challenging problem (Levitin and Ben-Haim, 2008). The main challenge of SRA is to provide best possible situational awareness to the decision makers (DM). Efficient SRA is essential and a valuable decision aid. SRA is an objective and preferably quantitative evaluation of security risks considering threats, vulnerabilities, and consequences. SRA is a technique for identifying, characterizing, quantifying, and evaluating the risk from an intelligent event. Many methods/tools of typical RA have been applied to support SRA. The basic methods for SRA can be categorized in two main categories as: qualitative SRA methods and quantitative SRA methods (Apostolakis, 2004; Cox et al., 2005).

In the qualitative SRA methods, the results are often shown in the form of a simple risk matrix where one axis of the matrix represents the probability and the other represents the consequences (Figure 1.1).

Likelihood	Consequence				
	Minor	Serious	Very serious	Major	Catastrophic
Very High					
High					
Medium					
Low					
Very Low					

Figure 1.1 : Risk matrix.

In the Figure 1.1 darker the colour of the cell, higher the risk is. The advantages of qualitative SRA methods are as follows (Cox et al., 2005):

- only a few qualitative judgments is required as inputs (ordered categorical labels such as “low,” “medium,” and “high”),
- the rating logic is transparent and easy to apply,
- calculations are reduced to simple categorizations of risk as outputs that can be communicated relatively easily to DMs.

The disadvantages of qualitative SRA methods are as follows:

- sufficient information to discriminate accurately between quantitatively small and quantitatively large risks is not provided,
- simple linguistic variables such as “High/Low” have the limitations in quantifying the risk and only represent subjective mental cognition adequately.

Quantitative SRA methods include quantifying and categorizing risks within the risk portfolio. When adequate data are available, quantitative SRA is preferred. Quantitative methods of RA to analyze the security risk are fairly limited. There is great uncertainty about the risk scenarios and contributing factors. Unfortunately, detailed quantitative data are frequently not available. There are two common quantitative methods: scoring methods and probabilistic methods.

In the typical quantitative SRA scoring methods, security risk is determined through the risk score which is defined as the product of the threat, vulnerability and consequence. The three factors threat, vulnerability and consequence are all evaluated using the ratings or scores. Typical scoring method based on Eq.1.1 produce ambiguous or mistaken security risk estimates because of the following reasons:

- Directly estimating scores for the security risk factors (Threat, Vulnerability, and Consequence),
- Intrinsic subjectivity and ambiguity of security risk factors,
- Not modelling uncertainty suitably in the light of available information and experience,
- Inability to use risk-scoring results to optimally allocate defensive resources,
- Ignoring intelligent planning and adaptation.

The other most common quantitative SRA method is probabilistic RA (PRA) (Ezell et. al., 2010; McGill, 2007; Kirchsteiger, 1999). In the PRA, probability theory is the foundation of contemporary risk analysis. PRA which is based on probability theory

emphasizes random uncertainties and requires statistical data about each parameter. Probabilistic method is an effective tool to study risk when a great amount of data can be collected. For PRA, threat is measured by the frequency of the intentional attack, vulnerability is measured by the probability that the attack defeats the security of the system, and consequence is the expected loss if the system fails. For example, assume that based on the data available, Threat is modelled with a normal probability distribution with mean 0.005 per year and standard deviation 0.0008 per year. Vulnerability is modelled with a lognormal probability distribution with mean 0.06 and standard deviation 0.02. Consequence is modelled with a uniform probability distribution with minimum 1 million and maximum 7 million (mean 4 million) Liras (L) per year. Using convolution of probability distributions under multiplication or Monte Carlo simulation, the expected value (mean) of risk can be calculated as L per year.

Difficulties of PRA are as follows:

- Many of the events in the intentional attack are fairly rare events and their probabilities cannot be estimated from data and in terms of one single probability,
- Probability is not valid for non repeatable events,
- Expert opinion is frequently employed as a method of eliciting probability estimates, but this is unreliable in the case of rare events,
- When there are very few data, the end result is very strongly influenced by the assumed prior distribution.

In this section limitations of conventional models/theories are discussed and the results of qualitative and quantitative RA systems are evaluated.

1.2 Aim and Objective

It is clear that analyzing the security risk of intelligent acts with the potential for severe consequences considering vulnerabilities requires methods of analysis that systematically and rigorously quantify uncertainties. There is a need for a realistic quantification of security risk factors. The quantitative description of security risk is affected by the accuracy of the estimates of the likelihood of events, vulnerability of assets and the quality of the consequence study. This thesis proposes a quantitative SRA framework that offers a methodology for assessing the security risk of critical

facilities. The purpose of the proposed framework is to support effective decision making to SRA for defending critical facilities against malevolent attacks. This thesis is about a description of the nature of security risk, a security risk assessment methodology, information requirements to security risk, and recommendations for successful implementation. There are many challenges in the details of SRA. The main research questions are as follows:

- How to measure/quantify/represent security risk factors: Threat likelihood, Vulnerability, Consequence, and Security risk?
- How to aggregate threat likelihood, vulnerability and consequence for SRA?
- What is the appropriate uncertainty model for SRA?
- How to improve SRA decisions?

The main objectives of this study are to propose a new realistic framework to SRA process for incorporating uncertainties using required concepts into conventional RA frameworks, to understand the security risks involved that might affect the critical facility and to demonstrate how proposed SRA can help in decision-making considering research questions.

1.3 Theory, Methodology and Data

The three fundamental factors used to assess the security risk of threat scenario are threat, vulnerability and consequence (Eq.1.1). SRA focuses on quantification of these factors and aggregation of them for SRA. In order to accomplish SRA; four different models are developed for each factor of the SRA framework as Threat Assessment Model (TAM), Vulnerability Assessment Model (VAM), Consequence Assessment Model (CAM), and Security Risk Evaluation Model (REM) (Figure 1.2).

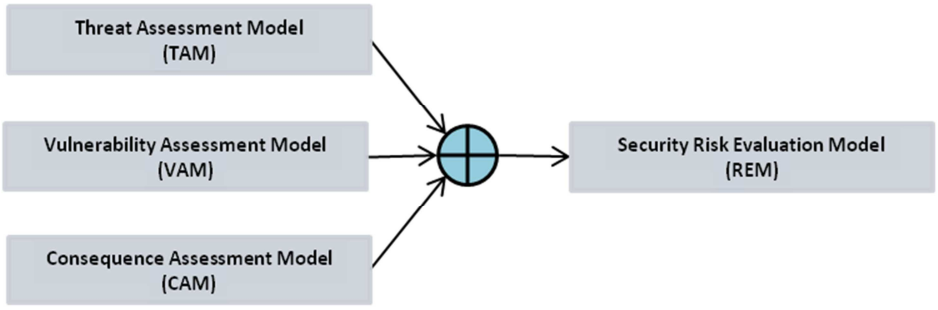


Figure 1.2 : Models of security risk assessment framework.

- Threat Assessment Model (TAM): TAM identifies threats of a critical facility and estimates their likelihoods. The threat assessment also generates the initiating events, possible threat scenarios, for the other models of SRA framework (Chapter 2).
- Vulnerability Assessment Model (VAM): VAM identifies and quantifies the weakness of the critical facility as a system, system functions and system components, and determines the most critical functions and components by simulating the system behaviour (Chapter 3).
- Consequence Assessment Model (CAM): CAM estimates the expected magnitude and type of loss (e.g., deaths, injuries, or property damage) associated with a threat scenario given adversary success for a critical facility. This model involves quantification of the likely loss or damage due to anticipated threat scenarios (Chapter 4).
- Security Risk Evaluation Model (REM): REM aggregates the outputs of TAM, VAM and CAM for evaluating the security risk of a critical facility (Chapter 5).

Each developed model in SRA framework proposes an approach for quantification of corresponding security risk factor. Quantification of security risk factor means that the factor is represented by a mathematical parameter that embodies enough information supported by the evidence for estimating the future values.

Proposed SRA framework has been studied in three dimensions: theoretical framework, methodological framework and information processing framework and described in the following sections.

1.3.1 Theoretical framework

The choice of the appropriate uncertainty theory is a critical modelling decision and context dependent. In typical RA, no distinction is traditionally made between different types of uncertainty for the factors and in the literature generally uncertainty has been addressed using only one of the uncertainty theories within the computations. Few studies have considered the issue of integrating different modes of representation of uncertainty in a single computational procedure (Guyonnet et al., 2003).

There are limitations in using only one uncertainty theory to quantify the security risk factors in a framework because security risk factors involve different types of

uncertainty stem from technical, non technical or social sources of the concerned risk type: security risk. To quantify the any security risk factor, it is first necessary to choose the appropriate uncertainty theory. The appropriate uncertainty theory used to describe studied security risk factor should obviously be compatible with the features of this factor, by the type of required input information, by the quality of required output information and by the axiomatic assumptions about the cause of uncertainty. Therefore, choosing an uncertainty theory is important because:

- An uncertainty theory has to be appropriate to the available quantity and quality of input information,
- An uncertainty theory determines the type of information processing applied to available information,
- An uncertainty theory determines the output.

Research advances in uncertainty modelling and decision making have produced new opportunities for representing and processing information. Most of the established theories and methods for uncertainty modelling are focused on specific types of uncertainty and they also require specific types or qualities of information depending on the type of information processing they use. There is not any single method or theory which is sufficient to model all types of uncertainty equally well.

Since parameter uncertainty is a major aspect of SRA, in quantifying the security risk, only one uncertainty theory is not enough because of different nature of security risk factors. In order to handle various types of possible uncertainties that occur in the implication/application of SRA, this thesis proposes a framework to represent each factor with different uncertainty theory for SRA. The proposed uncertainty modelling strategy for SRA is depicted in Figure 1.3 based on the characteristics of the uncertainty on security risk factors.

This thesis investigated the uncertainty affecting security factors in SRA and the use of probability theory, fuzzy set theory, Dempster-Shafer theory of evidence (DST) and other uncertainty theories for SRA. The possible application of different uncertainty theories to the quantification of SRA factors are explored and described in the following chapters.

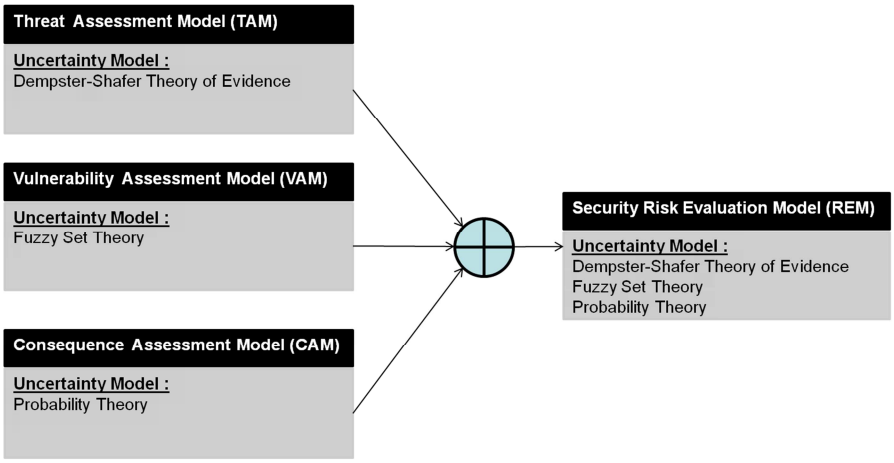


Figure 1.3 : Theoretical framework.

1.3.2 Methodological framework

On methodological dimension, proposed SRA framework consists of four models that apply several methodologies consistent with each other for the quantification of corresponding security risk factor. The proposed multi methodological modelling strategy for SRA is depicted in Figure 1.4 based on the characteristics of the special challenges of security risk factors.

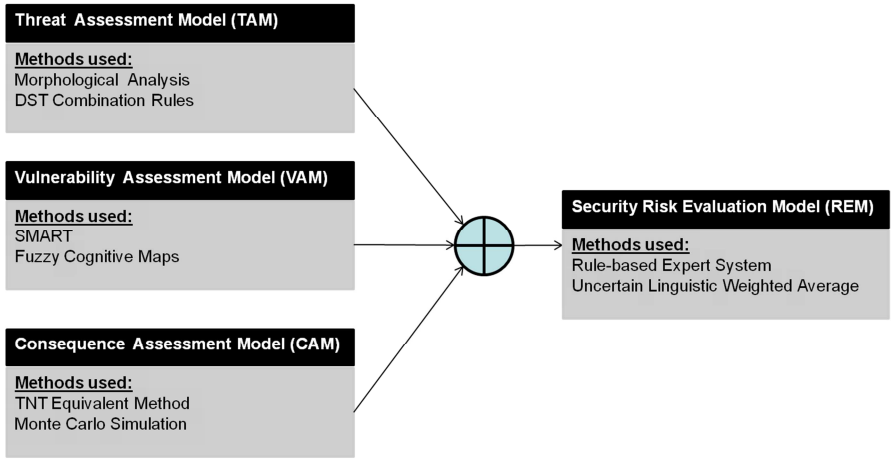


Figure 1.4 : Methodological framework.

Methodologies relevant to address the special challenges of security risk factors that can be applied to the quantification of security risk factors are investigated. These include problem structuring methods (PSM) such as Morphological Analysis (MA), multiple criteria/attribute decision making (MCDM) techniques such as Simple Multi-Attribute Rating Technique (SMART), data integration methods and evidence

combination techniques (combining data collected from multiple sources with different sampling rates or data schemas to reach a conclusion) such as rule based expert systems, DST combination rules and Uncertain Linguistic Weighted Average (ULWA), and modelling and simulation techniques such as Trinitrotoluene (TNT) equivalent method, Fuzz Cognitive Maps (FCM) and Monte Carlo simulation. The possible application of these methodologies to the quantification of SRA factors are explored and described in the following chapters.

1.3.3 Information processing framework

On information processing dimension, the factors must be represented in a way that is consistent with the resolution of data/information at hand and the information at hand must be structured in a suitable form as input to SRA. The input and output information requirements must be understood to support meaningful analysis of the security risks.

The available input information in SRA process can be very different in nature for security risk factors. The input data may be different both in type and in scale. It can be qualitative and quantitative, can be incomplete, imprecise (vague), unreliable, conflicting, overloaded. So, there is a need to establish a framework that provides a basis for synthesis across multidimensional information of varying quality. The available information is neither ignored nor exaggerated.

The historical data for SRA are limited and sometimes meaningless because of the characteristic of intelligent events in security risk. Both linguistic data and incomplete information are inevitable in SRA. When dealing with security risk, two extremes are avoided: reducing everything to inappropriate numerical forms and reducing everything to plain language rejecting technical and quantitative data. Because of lack of complete information, intuition and judgement still play major role in SRA. Methods for extracting reliable knowledge from experts and representing knowledge in more suitable form are investigated and developed.

The proposed information processing strategy for SRA is depicted in Figure 1.5 based on the characteristics of the input information available and the quality of required output information.

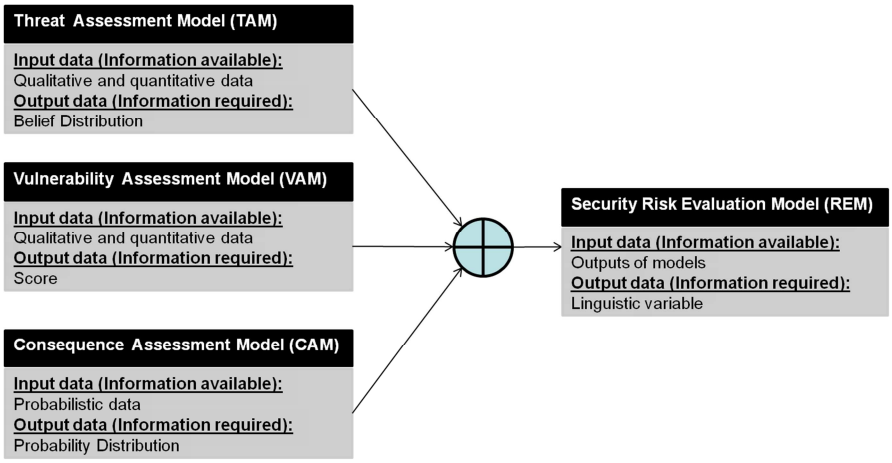


Figure 1.5 : Information processing framework.

Since data for the security parameter in each model are obtained via different uncertainty models, data for the parameters in each of these models can be obtained in different forms, and can be specified in terms of linguistic variables, point estimates, means and standard deviations, intervals, probability distributions, fuzzy numbers or belief distributions. The handling various types of input and output information of SRA factors are explored and described in the following chapters. An illustrative example is also provided to demonstrate an application of developed models for a typical critical facility. The developed models as described in following chapters are applied to a hypothetical Airport X to discover threats, vulnerabilities, consequences and security risks for improving its site security (Figure 1.6). A typical airport is decomposed to the dimensions of functions, critical infrastructures and key infrastructure elements. Modern airports with their runways, taxiways, aprons, passenger terminals, ground handling and flight navigation equipment are very complex facilities (Ashford et al., 1997). Simply, the mission of an airport is to land, to unload payload, to load payload and to take off aircrafts. When the security requirements are considered against the possible malevolent attacks, the challenge of SRA for an airport becomes very complicated. Therefore, it is thought that an airport case can be an interesting example. Note that all the values used throughout this thesis are purely generic and notional.

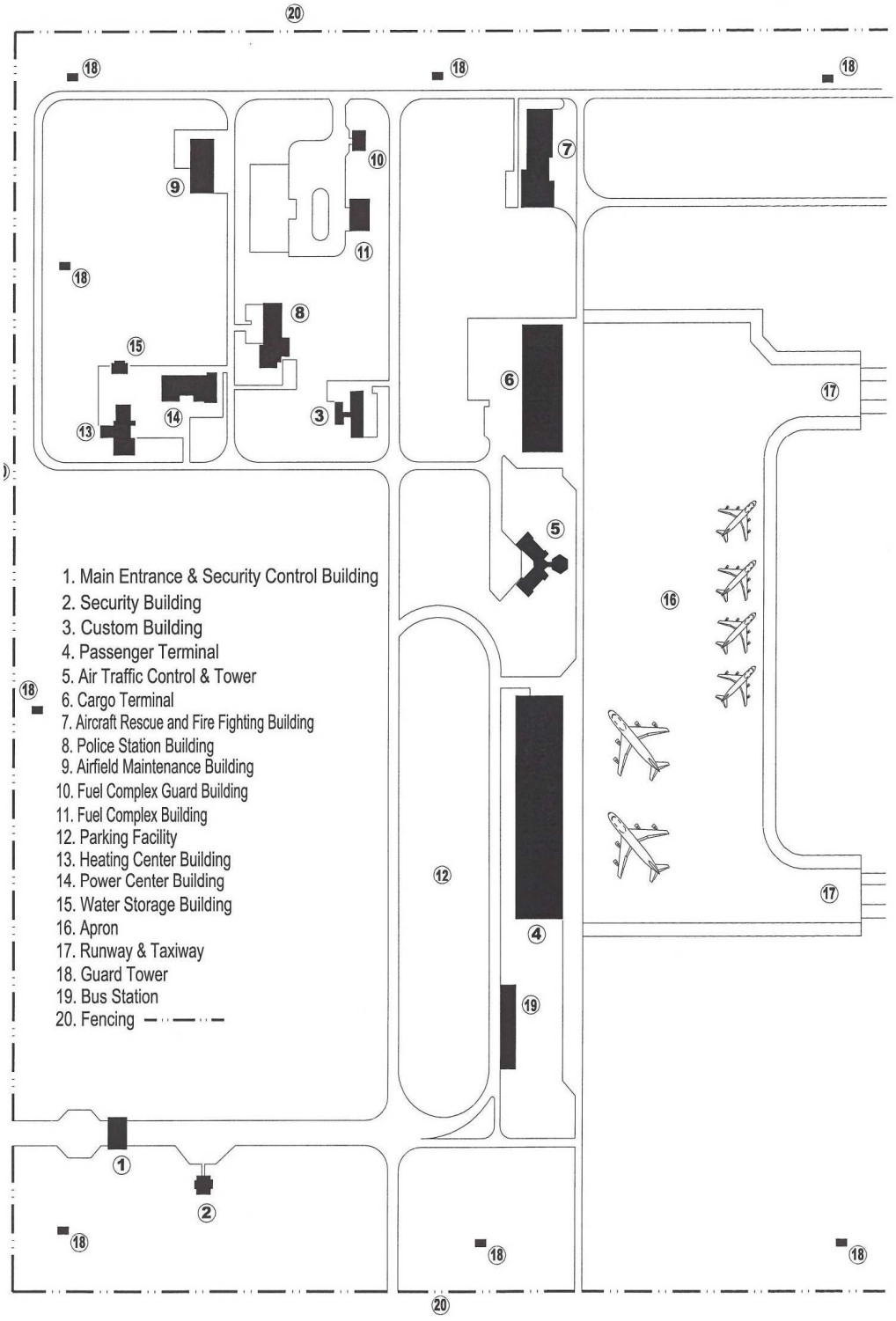


Figure 1.6 : Sketch of airport X.

2. THREAT ASSESSMENT MODELLING

2.1 Introduction to Threat Assessment

Critical facility threat assessment is considered to be the most difficult challenge in security risk assessment (SRA). In the security field, a threat is an intelligent event that is defined as any human caused act, entity, event or phenomenon with the potential to cause harm or damage to a critical facility by adversely changing its state. In other words, a threat is a human caused intelligent event of undesired consequence and different from random events. In the system perspective, the critical facility, such as an airport, dam, governmental facility, harbour, nuclear power plant, oil plant etc., can be defined as a system that relies on a group of different physical entities as system components which are attractive targets subject to threats. Unlike accidental failures, human caused threats are deliberate, innovative, and unpredictable acts against the targets of critical facility. Forecasting threats are difficult because adversaries will continue to improve tactics and enhance their capabilities according to changing conditions. Before the security risk is assessed, threats and their likelihoods must be identified and quantified. Therefore, threat assessment is the task of identifying threats and estimating their likelihoods, and involves two sub-phases: threat identification and threat likelihood estimation, which are described in the following sections (Figure 2.1).

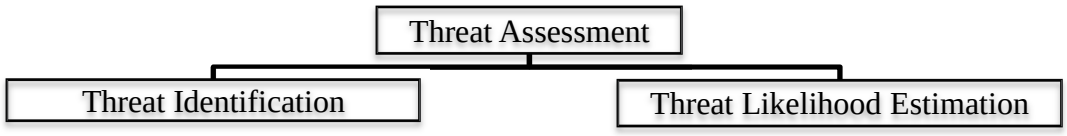


Figure 2.1 : Threat assessment.

The aim of this chapter is to present a realistic approach to quantify the likelihood of threats by identifying them based on the appropriate uncertainty model and supplementary methods for a critical facility considering both information at hand (input information) and information requirements of DMs (output information). The proposed approach, called evidence based Morphological Analysis (EMA) model, is

based on Dempster-Shafer theory of evidence (DST) and Morphological Analysis (MA) methodology. EMA model incorporates DST with MA for threat assessment of a critical facility in this study. The proposed approach is presented step by step and applied to a simple case study on airport threat assessment. The results show that EMA can be used to reason about threat assessment by providing adequate precision. After reviewing the existing approaches and the factors that influence the threat identification and likelihood estimation, the remainder of this chapter is organized as follows: In Section 2.2, theoretical background information for the proposed approach is represented. The proposed EMA model and its process flow are introduced in Section 2.3. The illustrative application of the proposed approach is performed over an airport case study in Section 2.4. This section also examines the utility of findings and discusses the analysis results. Conclusions and further issues are addressed respectively in the final section.

2.1.1 Threat identification

Threat identification sub-phase identifies threats that a critical facility may suffer by developing an exhaustive set of plausible threat scenarios based on the susceptibilities of its possible targets to possible attack profiles considering information on the intentions and capabilities of the attackers, targets and weapon delivery systems. Threat identification is the basis for identification, filtering and prioritizing of threat scenarios on which concentration is needed. For developing plausible threat scenarios, extensive involvement of security experts is required. The aim is to develop a complete set of plausible threat scenarios which are bounded in terms of the intentions and capabilities of the attackers. The development of threat scenarios is different because of the intelligent attacker. An examination of historical data is useful when identifying possible threat scenarios, but it is also required to identify possible threat scenarios that have never been happened in the past.

Since development of scenarios is critical for threat identification, a method for developing threat scenarios is required. In the literature, a variety of tree structures are often used to develop scenarios. Tree structures are important tools for exploring the scenario space, analyzing uncertain events and defining scenarios (Harris, 2004). Tree structures can be categorized in two types: event trees or fault trees that display functional and logical relationships among events. Given a set of initiating events, if

the structuring of scenarios is done by identifying succeeding events and tracing the response of a system from an initiating event to different possible end-states, scenarios constructed in this way form an event tree (Andrews and Dunnett, 2000). Each path through this tree represents a scenario and ends up at an end state started by an initiating event. Therefore, an event tree is a cause-and-effect representation of logic. Given an end-state, if the structuring of scenarios is done by projecting backwards to determine the potential scenarios that could cause the end-state, scenarios constructed in this way form a fault tree (Ericson, 1999). A fault tree starts with the end-state and attempts to determine all of the contributing system states. Therefore, fault trees are effect-and-cause representations of logic. An event tree is developed by inductive reasoning while a fault tree is based on deductive reasoning. In the literature, event trees and fault trees have been used to identify threat scenarios in several studies (Ezell et al., 2001; Rosoff and von Winterfeldt, 2007). But, tree structures as a hierarchical technique quickly become difficult to handle because of the wide variety of possible scenarios. Proposed technique must be fast enough to quickly analyze a wide range of plausible scenarios with modest computational effort.

In this study, MA is used for threat identification. The fundamentals of MA and reasons for using MA are described in the following sections.

2.1.2 Threat likelihood estimation

Threat likelihood estimation is the most uncertain aspect of the SRA problem. As threat scenarios are about what will happen, threat likelihood is about how likely it is to happen. At this sub-phase, threat scenario likelihoods are determined. The critical research question is “Which interpretation of likelihood is the most informative and is the preferred way of capturing and quantifying the state of knowledge about the likelihood of a defined threat scenario for a critical facility?” Quantification of likelihood means that the threat likelihood is represented by a mathematical parameter that embodies enough information supported by the evidence for estimating the future occurrences of intentional attacks. To quantify the threat likelihood, it is first necessary to choose the appropriate uncertainty model and define the concept of likelihood. Modelling uncertainty is one of the most critical modelling decisions (Zimmermann, 2000). The choice of the appropriate uncertainty model is context dependent. The appropriate uncertainty model used to describe

studied situation should obviously be compatible with the features of this situation, by the type of required input information, by the quality of required output information and by the axiomatic assumptions about the cause of uncertainty. Therefore, choosing an uncertainty model is important because:

- An uncertainty model has to be appropriate to the available quantity and quality of input information,
- An uncertainty model determines the type of information processing applied to available information,
- An uncertainty model determines the output.

There are two main types of uncertainty: aleatory uncertainty and epistemic uncertainty. Epistemic uncertainty is referred to as reducible, subjective and state-of-knowledge uncertainty and aleatory uncertainty is referred to as random, irreducible and stochastic uncertainty (Helton, 1997; Oberkampf et al., 2004).

Many researchers have investigated how to deal with both uncertainties and there exist a considerable number of theories, methods or paradigms to model uncertainty. Some commonly used uncertainty models are as follows: probability theory (Laplace, 1812; Kolmogorov, 1950), fuzzy set theory (Zadeh, 1965), possibility theory (Zadeh, 1978; Dubois and Prade, 1988), and Dempster-Shafer theory of evidence (Dempster, 1967; Shafer, 1976). But, there is not any single method or theory which is sufficient to model all types of uncertainty equally well. Each of these theories makes assumptions about available information, it contains a certain calculus by which these information are processed and certain measures of uncertainty. A specific uncertainty model should not be used if its mathematical operations require a higher level of information than that on which the available information is provided. This is very important when applying those models. Uncertainty models transform input information to output information. Underestimation and wrong interpretation of uncertainty is an important mistake. Therefore, the choice of appropriate uncertainty model for threat likelihood estimation is crucial.

In probabilistic risk assessment (PRA), quantitative interpretations of likelihood are frequency, probability, and probability of frequency (Ezell et. al., 2010; Kirchsteiger 1999). If the event happens repeatedly, its likelihood can be expressed as frequency

like in occurrences per day, per year, per trial, etc. If the event happens either once or not, its likelihood can be quantified in terms of probability. If the event happens repeatedly and has a frequency, but the numerical value of that frequency is not fully known, its likelihood can be expressed as a probability of frequency. The most appropriate mathematical representation of likelihood is probability theory when the given information is perfect and complete. It is difficult to obtain precise relation between events and their likelihoods. The PRA requires having all the information on the probability of all events. When such information is not available, the uniform distribution function is used. Uniform distribution function states that all events in a given sample space are equally likely. Because of the axiom of additivity (where all probabilities that satisfy specific properties must sum to 1) in the probability theory, if it is believed that a likelihood of an event A is 0.25, it is necessarily believed that likelihood of not event A (complement of A) is 0.75. This is a strict assumption for threat likelihood. Even if there is a historical data and predetermined probability function fits the limited historical data well, the threat likelihood estimation results may not be good in practice because of the human factor in deliberate and adaptive events of security risk. In case of partial ignorance, the use of a single probability measure introduces information that is in fact not available. This may seriously bias the outcome of a threat assessment in a non conservative manner. Probability theory is an appropriate uncertainty theory for analysis of random events. But, is randomness one of threat likelihood nature? Although some threat has never happened, it will be possible in the future. Threat likelihood estimation involves uncertainty associated with predicting an event in the future. Zadeh's egg example illustrated the difference between probability and possibility simply by the following example (Zadeh, 1978). Consider "Hans ate X eggs for breakfast" with X taking values in u = {1, 2, 3, 4, 5, 6, 7, 8} (Table 2.1).

Table 2.1: Egg example.

u	1	2	3	4	5	6	7	8
$Possibility_x$ (u)	1	1	1	1	0.8	0.6	0.4	0.2
$Probability_x$(u)	0.1	0.8	0.1	0	0	0	0	0

As shown in the Table 2.1, a high degree of possibility does not imply a high degree of probability, nor does a low degree of probability imply a low degree of possibility. But, a high degree of probability implies a high degree of possibility and low degree of possibility implies low probability. If an event is impossible, it is bound to be

improbable. This is called Zadeh's possibility-probability consistency principle (Zadeh, 1978). Threats are also a class of events that may have a probability of zero but may not be impossible. Although something has never happened, it will be possible in the future.

Fuzzy logic based approaches have been extensively used to model vagueness and ambiguity, but it can not deal with such uncertainties as incomplete, imprecise and missing information (ignorance). Vagueness is uncertainty about the classification of a known event. For example, Hans is 22 years old, but it is said that Hans is young without the precise definition of young. At this example, the word young is vague and can be addressed by using fuzzy set theory.

The threat is chosen and executed for a reason by the attacker. A threat, intentional attack for a critical facility, is neither random event nor vague event and uncertainty associated with such intelligent event involves epistemic uncertainty rather than aleatory uncertainty. The threat likelihood parameter must also be represented in a way that is consistent with the information at hand. For threat likelihood estimation, it is not possible to obtain a measurement from experiments and the input information is commonly obtained from expert elicitation. Threat likelihood is evaluated based on experience and judgement. The input information for threat likelihood is commonly expressed in qualitative terms and frequently described using linguistic variables. There is a significant body of knowledge in qualitative or linguistic form for determining threat likelihood and this knowledge has to be captured.

In this study, DST is used for uncertainty modelling and the input data for threat likelihood are represented by DST variables due to epistemic uncertainty. The fundamentals of DST, reasons for modelling uncertainty by DST, and how DST is applied for threat likelihood estimation within MA is described in the following sections.

2.2 Theoretical Background for Threat Assessment Modelling

In this section, theoretical background information on Morphological Analysis (MA) and fundamentals of Dempster-Shafer theory of evidence (DST) are presented, respectively.

2.2.1 Morphological analysis

MA, developed by Fritz Zwicky in 1969, is a qualitative modelling method for structuring parameter space of the multidimensional non-quantifiable problems by defining relationships between the parameters on the basis of internal consistency (Zwicky, 1969). As a qualitative problem structuring method, MA has been applied to complex social, organizational and technical problem fields for the scenario planning, strategy formulation, policy development, etc. (Sharif and Irani, 2006a;b; Ritchey, 1998; 2009).

MA begins by forming a morphological field and corresponding cross-consistency assessment (CCA) matrix in MA's terms. A morphological field, matrix of the state of all conditions in the system, is constructed by identifying and defining the parameters of the problem and assigning each parameter a range of relevant values in a multidimensional matrix. A configuration contains one value from each of the parameters and represents a particular state, solution or scenario in the problem. The next step in the MA is to examine the internal relationships between the parameters and reduce the morphological field by eliminating all mutually contradictory conditions. This is achieved by a process of cross-consistency assessment in the CCA matrix where all of the parameter values in the morphological field are evaluated pair wise with the other parameter values by defining pairs that can not coexist and removing the configurations that contain a single illogical pair. The exponential growth to unmanageable numbers of permutations is decreased by discarding illogical pairs through a process of cross-consistency assessment in the CCA matrix. By doing this, solution space of the problem is determined. The solution space consists of the subsets of configurations that satisfy the condition of internal consistency.

In MA different from event trees and failure trees, structuring of a configuration is done by using logical relationships instead of casual relationships. The important feature of MA is to reduce the solution space. The total number of configurations (possible or not) is the product of the number of values under each parameter. The total number of configurations grows exponentially with each new parameter but the number of pair wise relationships between parameters grows only as a quadratic polynomial that is proportional to the triangular number series (Ritchey, 1998; 2009).

Therefore, even a morphological field involves many configurations, fewer number of pair wise evaluations is always required than the total number of configurations in order to create solution space. Advantages of MA are as follows:

- The solution space of any given problem can be derived systematically,
- New configurations or relations that is not so evident can be discovered more easily,
- Impossible configurations can be screened rapidly,
- Multi-dimensions in columns can easily be represented by morphological field and MA matrix structure helps to keep the solution space organized, accessible and traceable even at large sizes,
- New parameters and new parameter values can easily be added, and new relations can easily be updated.

But, there is no mechanism to address the issue of how to deal with incomplete, imprecise and ignorance in MA, which is essentially inherent and inevitable in expert judgements. Pair wise evaluations can take different forms instead of binary decision to determine the strength of the logical relations between the parameter values as proposed in this study.

In this study, MA is used for the purpose of the threat identification because MA is fast enough to quickly analyze a wide range of plausible threat scenarios with modest computational effort.

2.2.2 Dempster-Shafer theory of evidence

The Dempster-Shafer theory of evidence (DST) is an alternative theory for the mathematical representation of uncertainty (Dempster, 1967; Shafer, 1976). There are many practical applications of DST in the literature such as artificial intelligence, expert systems, pattern recognition, data fusion, etc. (Dempster et al., 2008). Applications of DST in typical risk assessment have been very limited because probabilistic methods are successful where a lot of experimental data and expert knowledge are available (Demotier et al., 2006).

The theory begins by defining the frame of discernment (FD), denoted by $\Theta = \{H_1,\ldots, H_N\}$, which is a collectively exhaustive and mutually exclusive set of

propositions or hypotheses. The power set, 2^{Θ}, is constructed from Θ which consists all subsets of Θ, including the empty set (Ø) and Θ itself i.e. $2^{\Theta} = \{\varnothing, \{H_1\}, ..., \{H_N\}, \{H_1, H_2\}, ..., \{H_1, H_N\}, ..., \Theta\}$.

DST uses three basic parameters, i.e., basic probability assignment (bpa), belief measure (Bel), and plausibility measure (Pls) to characterize the uncertainty in a belief structure. The bpa (m) which is a function $m: 2^{\Theta} \rightarrow [0,1]$ satisfying following axioms:

$$m(\varnothing) = 0 \; and \sum_{A \subseteq \Theta} m(A) = 1 \qquad \textbf{(2.1)}$$

where A is any subset of Θ ($A \in 2^{\Theta}$). The bpa for a given set A, m(A), measures the belief exactly assigned to A and represents how strongly the evidence supports A. The bpa's of all the subsets of Θ sum to unity and the bpa of Ø is 0. The bpa of Θ, m(Θ), is called the degree of ignorance. Each subset A with m(A)>0 is called a focal element and all the focal elements are called the body of evidence.

The belief measure (Bel) and the plausibility measure (Pls) are the functions associated with each bpa and defined by the following equations:

$$\text{Bel(A)} = \sum_{B \subseteq A} m(B) \qquad \textbf{(2.2)}$$

$$\text{Pls(A)} = \sum_{A \cap B \neq \varnothing} m(B) \qquad \textbf{(2.3)}$$

where A and B are subsets of Θ. Bel(A) represents the exact support to A. Pls(A) represents the possible support to A. The two functions are connected by the equation:

$$\text{Pls(A)} = 1 - \text{Bel}(\bar{A}) \qquad \textbf{(2.4)}$$

where $\bar{A}$ denotes the complement of A. The difference between the Bel(A) and Pls(A) describes the ignorance of the assessment for the set A (Figure 2.2).

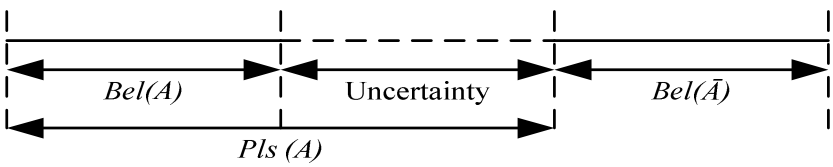


Figure 2.2 : Belief and plausibility.

[Bel(A), Pls(A)] constitutes the interval of support to A and can be interpreted as the lower and upper bounds of the probability to which A is supported due to lack of information. The precise probability of an event lies within the lower and upper bounds of Bel and Pls, respectively (Bel(A)≤P(A)≤Pls(A)). The wider the interval, the less informative it is. The measurements Bel, Pls, and probability will converge to a single probability when the information increased sufficiently (Bel(A)=P(A)=Pls(A)). The sum of all the Bel and the sum of all the Pls are not required to be 1 and therefore, both Bel and Pls are non-additive.

The other important aspect of DST is the combination rules that are the special types of aggregation methods for data obtained from multiple independent information sources. Detailed discussions on these rules can be found in the literature (Sentz and Ferson, 2002; Smets, 2007). These rules can be either conjunctive rules (AND-based on set intersection) or disjunctive rules (OR-based on set union) from a set theoretic standpoint. Two most common combination rules, both one conjunction based rule and one disconjunction based rule, are used and compared in this study: the Yager's modified Dempster's rule (Yager's rule) and the Dubois and Prade's disjunctive consensus rule (DP's rule) (Dempster, 1967; Yager, 1987a;b; Dubois and Prade, 1992).

$$m_1 \oplus_{DP} \ldots \oplus_{DP} m_i \oplus_{DP} \ldots \oplus_{DP} m_n(A) = \begin{cases} \sum_{\cup_{i=1}^{n} A_i = A} m_1(A_1) * \ldots * m_i(A_i) * \ldots * m_n(A_n) & , A \neq \varnothing \\ 0 & , A = \varnothing \end{cases} \quad \textbf{(2.5)}$$

$$m_1 \oplus_{Yager} \ldots \oplus_{Yager} m_i \oplus_{Yager} \ldots \oplus_{Yager} m_n(A) = \begin{cases} \sum_{\cap_{i=1}^{n} A_i = A} m_1(A_1) * \ldots * m_i(A_i) * \ldots * m_n(A_n) & , A \neq \Theta \\ \sum_{\cap_{i=1}^{n} A_i = A} m_1(A_1) * \ldots * m_i(A_i) * \ldots * m_n(A_n) + K & , A = \Theta \\ 0 & , A = \varnothing \end{cases} \quad \textbf{(2.6)}$$

$$K = \sum_{\cap_{i=1}^{n} A_i = \Phi} m_1(A_1) * \ldots * m_i(A_i) * \ldots * m_n(A_n) \quad \textbf{(2.7)}$$

where A_i's are propositions from different information sources, $m_i(A_i)$s are corresponding bpas, K represents bpa associated with conflict, and the symbol $\oplus$

represents operator of combination. The symbol $\oplus_{DP}$ represents DP's rule and the symbol $\oplus_{Yager}$ represents Yager's rule.

In the case of multiple information sources, two algebraic properties enable evidence to be combined in any order: commutativity and associativity, i.e. $m_1 \oplus m_2 = m_2 \oplus m_1$ and $(m_1 \oplus m_2) \oplus m_3 = m_1 \oplus (m_2 \oplus m_3)$. Therefore, commutativity and associativity of the combination rules are required for multiple information combinations. These algebraic properties are satisfied by each of the applied rules: the Yager's rule is both commutative and quasi-associative, and the DP's rule is both commutative and associative. These properties can be seen in Sentz and Ferson (2002).

Major difficulty in applying the DST is the computational complexity. There is no explicit function of the given imprecise information in DST like the probability density function. The significant difference of DST is that bpas are assigned to sets and subsets of sample space rather than mutually exclusive singletons as in probability theory. This implies an exponential increase in computational complexity. The subsets to which the bpas are assigned can be consonant (nested) or non consonant and continuous or discrete. Under the restriction that all the focal subsets are nested, Pls is referred to as possibility and Bel is referred to as necessity in possibility theory (Dubois and Prade, 1988).

DST is selected for the likelihood estimation because both epistemic uncertainty and aleatory uncertainty can be handled by the help of the flexibility of DST basic axioms. DST is also well suited for handling incomplete information without any additional assumptions as additivity. Lastly, DST combination rules allow aggregating different types of evidence obtained from multiple sources easily. Details of the application of DST within MA to likelihood estimation are described in the next section.

2.3 Evidence based Morphological Analysis Model

Likelihood estimation of complex events like intentional attacks in threat assessment is difficult to assess directly because it is not possible to obtain a precise measurement from experiments. Therefore, EMA model decomposes these events into simple relations and determine the overall event likelihood by assembling the

relations' likelihoods using DST combination rules. EMA model provides an efficient approach for breaking/making a large and complex assessment into a sequence of smaller and simpler relations that can be more easily addressed in a structured way.

The proposed EMA model incorporates DST with MA in this study. Different from typical MA applications, the strength of logical relations between the parameter values are not limited to binary (Yes or No) decisions since experts may express likelihood of existence of relation which is characterized by the linguistic evaluation grades that represent the qualitative expert assessments. Typical qualitative analysis of MA identifies all the plausible scenarios, whereas proposed EMA both identifies all the plausible scenarios and estimates the likelihood of plausible scenarios based on DST. The proposed model allows to express qualitative judgements using belief structures developed on the basis of DST and make full use of available information without information loss and exaggeration. A relation in MA may change when more information is get by time. Thus, the notion of time, t, is also introduced into the problem formulation.

The proposed model first identifies the parameters of the scenarios and defines a range of values for each parameter. Original FD is determined for evaluation of CCA matrix relations and bpas for evaluation of CCA matrix relations are assigned. Relations within MA are combined using belief structures that are aggregated to form the scenarios by two well-known DST combination rules: DP's rule and Yager's rule. Then, the belief intervals of all scenario likelihoods are calculated. The likelihoods of identified scenarios are ranked based on their belief intervals according to defined preference relation using bubble sort algorithm. The proposed approach consists of the following steps shown in Figure 2.3.

Step 1: Identify the parameters and define a range of values for each parameter

In this step, the scenario parameters are identified and a range of values for each scenario parameters are defined. Suppose in a morphological field there are L basic parameters and let be a set of parameters $A=\{A_1,\ldots, A_i,\ldots A_L\}$. A set of basic values for parameter A_i is defined as $A_i = \{a_1^i,...,a_k^i,...,a_{L(A_i)}^i\}$ where a_k^i is the kth value of the parameter A_i and $L(A_i)$ is the total number of the values of parameter A_i.

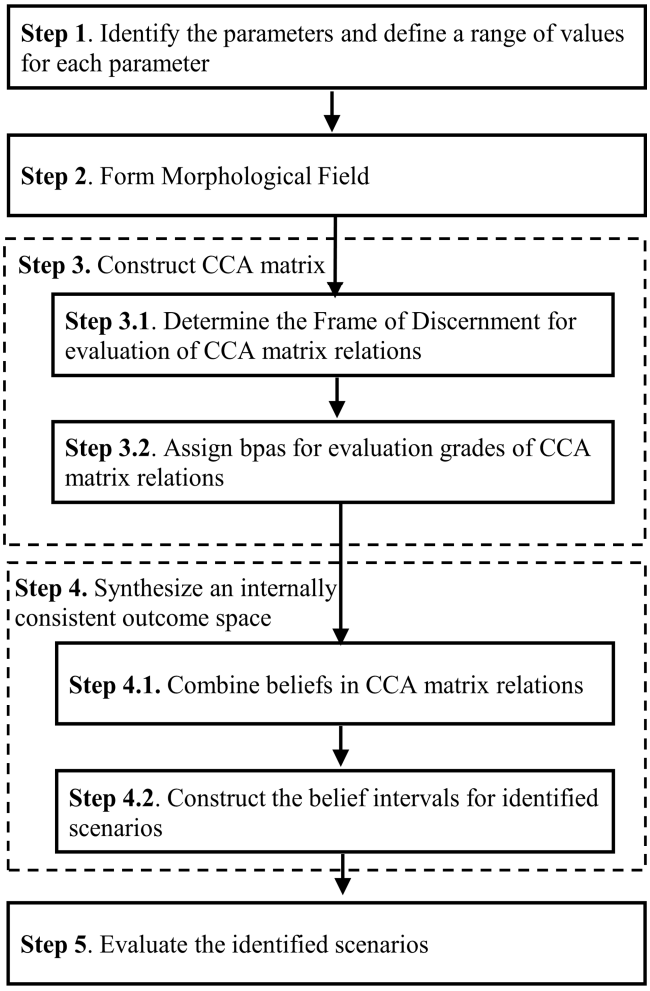


Figure 2.3 : The steps of EMA model.

Step 2: Form Morphological Field

Morphological field is formed as shown in Table 2.2.

Table 2.2: Sample morphological field.

Parameter A_1	**…**	**Parameter A_L**
a_1^1	. . .	a_1^L
. . .	. . .	. . .
. . .	. . .	$a_{L(A_L)}^L$
$a_{L(A)}^1$	. . .	

Step 3: Construct Cross-Consistency Assessment (CCA) Matrix

At this step, definition and representation of CCA matrix is done based on DST.

Sub-step 3.1: Determine the Frame of Discernment for evaluation of CCA Matrix relations

Determination of the FD is context dependent and very important. Since bpas are assigned to subsets of the FD in DST, this implies an exponential increase in computational complexity (Liu et al., 2007). The other point is that FD affects the way information captured. Therefore, FD is determined considering both information at hand and computational complexity in this study.

Qualitative judgement information given by security experts is essential to quantify likelihood. Security experts as in many fields tend to think in linguistic terms and usually give their subjective judgements linguistically by means of a set of evaluation grades. Different types of assessment information, such as complete and incomplete, precise and imprecise assessments, may be expressed as follows (Yang and Singh, 1994):

Assessment 1: Absolutely (100%) believe that explosive attack to target 1 is "Likely" expressed by DST format as {(Likely,1)};

Assessment 2: 70% believe that explosive attack to target 2 is "Likely" and 30% believe that it is "Highly Likely" expressed by DST format as {(Likely,0.7), (Highly Likely,0.3)};

Assessment 3: 80% believe that explosive attack to target 3 is "Likely" expressed by DST format as {(Likely,0.8)};

Assessment 4 : 90% believe that explosive attack to target 4 is between "Likely" to "Highly Likely" and 10% believe that "Extremely Likely" expressed by DST format as {(Likely-Highly Likely,0.9), (Extremely Likely,0.1)};

Assessment 5: No judgement, which means experts can not provide an assessment for likelihood of relation under consideration, is expressed by DST format as {(Θ,1)}.

In the above statements, the input is given as a distribution using linguistic terms with the belief degrees (30%, 70%, etc.) based on subjective judgments. Each belief degree is the individual bpa of the input to the evaluation grade. When all the belief degrees are summed to one in an assessment, the assessment is said to be complete; otherwise, it is said to be incomplete. Assessment 1,2 and 4 are complete while assessment 3 is incomplete. No judgement is referred to as total ignorance as in assessment 5. Total ignorance corresponds to whole domain of likelihood being possible. The decision maker may not always be 100% sure that the state of a relation is exactly confirmed to one of the evaluation grades since FD, Θ, consists all

evaluation grades. Incomplete assessments may result from lack of data, unavailable data, partially known data or the inability of experts to provide valid and accurate information. For handling incomplete information, the Θ is taken as a focal element by assuming that the unknown evidence may let all evaluation grades have equal evaluation. For example, in assessment 3 the missing 0.2 represents the degree of ignorance and is assigned to Θ. The decision maker also may not always be confident enough to provide subjective assessments to individual grades and may assess beliefs to subsets of adjacent grades, intervals, like in assessment 4. In assessment 4, the individual grades are extended to include interval grades such as "Likely-Highly Likely".

In order to reduce the computational complexity, all of the CCA matrix relation likelihoods between each scenario parameter are assessed on the basis of H_{pq} (p,q=1,…,N) evaluation grades where H_{pp} is an individual evaluation grade, and H_{pq} for p=1 to N and q=p+1 to N-1 is the interval evaluation grade between H_{pp} and H_{qq} (p<q,q=2,...,N). H_{pp} (p=1,...,N) are required to be mutually exclusive. Therefore, a set of evaluation grades for relation likelihood, FD, is denoted by

$$\Theta = \{H_{pq}, \mathrm{p} = \mathrm{q}, \mathrm{p} = 1, ..., \mathrm{N}\} \quad \textbf{(2.8)}$$

Θ constitutes a FD and interval evaluation grades are special subsets of mutually exclusive individual evaluation grades in the terminology of DST. H_{11} and H_{NN} are set to be the worst and the best grades, respectively, and H_{p+1p+1} is to be preferred to H_{pp} among evaluation grades.

In this study, uncertain subjective judgments, such as complete and incomplete, precise and imprecise assessments, for evaluation of CCA matrix relation likelihoods are acquired using statements similar to statements 1-5 where H_{pq} represents an evaluation grade to which relations between each scenario parameter in MA may be assessed and (H_{pq}, $m(H_{pq})$) represents the input information.

Sub-step 3.2: Assign bpas for evaluation grades of CCA matrix relations

In the proposed EMA model, the relations among scenario parameters in CCA matrix are evaluated by assigning bpa to each linguistic evaluation grade and/or linguistic interval evaluation grades. Likelihood bpa assignments are based on subjective judgements because of the limited numeric data, and human judgement is needed to

weigh alternative interpretations of whatever data available. It is assumed that group of experts provide consensus evaluation for each relation. Group decision making techniques can be applied but beyond the scope of this study.

The Cartesian product of any two parameters in CCA matrix, A_i and A_j is determined as:

$$A_i \text{ X } A_j = \{(a_k^i, a_l^j) \mid a_k^i \in A_i,\ a_l^j \in A_j\} \quad \textbf{(2.9)}$$

which forms ordered pair of every $a_k^i \in A_i$ with every $a_l^j \in A_j$. The strength of relationship between ordered pairs of elements in typical MA is measured by the characteristic function, denoted χ, where a value of unity is associated with complete relationship and a value of zero is associated with no relationship as follows:

$$\chi_{A_i \text{ X } A_j}(a_k^i, a_l^j) = \begin{cases} 1 & , \quad (a_k^i, a_l^j) \in A_i \text{ X } A_j \\ 0 & , \quad \textit{otherwise} \end{cases} \quad \textbf{(2.10)}$$

However, in proposed approach the strength of relationship between ordered pairs of elements is measured by the following DST characteristic function as:

$$\chi_{A_i \text{ X } A_j}(a_k^i, a_l^j) = \begin{cases} m_t(H_{pq} / R_{ij}(a_k^i, a_l^j)), & (a_k^i, a_l^j) \in A_i \text{ X } A_j, H_{pq} \in 2^\Theta \\ 0 & , \quad \textit{otherwise} \end{cases} \quad \textbf{(2.11)}$$

where $m_t(H_{pq} / R_{ij}(a_k^i, a_l^j))$ expresses a bpa assigned to pair (a_k^i, a_l^j) from kth value of A_i and lth value of A_j confirmed to H_{pq} at time t. Therefore, each relation in proposed MA at time t is defined by the following expression:

$$R_{ij}^t(A_i, A_j) = \{(a_k^i, a_l^j) \mid m_t(H_{pq} / R_{ij}(a_k^i, a_l^j)) > 0,\ a_k^i \in A_i,\ a_l^j \in A_j, H_{pq} \in 2^\Theta\} \quad \textbf{(2.12)}$$
$$, i \neq j, i, j = 1, .., L$$

The belief structure of each relation $(a_k^i, a_l^j) \in R_{ij}^t(A_i, A_j)$ at time t can be defined as follows:

$$S_t(a_k^i, a_l^j) = \{(H_{pq}, m_t(H_{pq} / R_{ij}(a_k^i, a_l^j)))\} \quad , (a_k^i, a_l^j) \in R_{ij}^t(A_i, A_j), H_{pq} \in 2^\Theta \quad \textbf{(2.13)}$$

For example, in Table 2.3 belief structure for $(a_1^1, a_1^L) \in R_{1L}^t(A_1, A_L)$ at time t is $S_t(a_1^1, a_1^L) = \{(H_{24}, 0.5), (H_{11}, 0.5)\}$.

Table 2.3: CCA matrix.

		Parameter A_1			**Parameter …**			**Parameter**		**A_L**
		a_1^1	…	$a_{L(A_1)}^1$	…	…	…	a_1^L	…	$a_{L(A_L)}^L$
Parameter …	…									
	…									
	…									
Parameter A_L	a_1^L	$\{(H_{24},0.5),(H_{11},0.5)\}$								
	…									
	$a_{L(A_L)}^L$									

Step 4: Synthesize an internally consistent outcome space

Sub-step 4.1: Combine beliefs in CCA matrix relations

If a morphological field is defined by L basic parameters, there will be C_2^L relations in CCA matrix and each scenario is defined as a unique combination of relations in CCA matrix. Therefore, each relation considered as different information source and fused by using DST combination rules in order to produce an aggregated likelihood estimation of the scenarios. The relations, as different information sources, provide different assessments for the same FD and the aggregation among the relations produces the scenarios. The beliefs of relations in CCA matrix is aggregated using the DP's rule (Eq. 2.5) and the Yager's rule (Eq. 2.6) as follows:

$$m_t(H_{pq} / T(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)) = \sum_{\substack{ij\in C_2^L \\ k,l\in\{\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^M\},k\neq l}} \oplus_{DP/Yager}\, m_t(H_{pq} / R_{ij}(\mathrm{a}_k^i,\mathrm{a}_l^j)) \qquad ,\forall H_{pq} \tag{2.14}$$

where the symbol $\oplus$ represents operator of combination: the symbol $\oplus_{DS}$ represents DP's rule and the symbol $\oplus_{Yager}$ represents Yager's rule. Therefore, each scenario in proposed MA at time t is defined by the following expression:

$$\mathrm{T}_t(A_1,...,A_L) = \{(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L) \mid m_t(H_{pq} / T(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)) > 0,\ \mathrm{a}_\cdot^1 \in \mathrm{A}_1,...,\ \mathrm{a}_\cdot^L \in \mathrm{A}_L, H_{pq} \in 2^\Theta\} \tag{2.15}$$

The belief structure of each scenario $(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L) \in \mathrm{T}_t(A_1,...,A_L)$ at time t can be defined as follows:

$$\mathrm{S}_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L) = \{(H_{pq}, m_t(H_{pq} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)))\}, \forall(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L) \in T_t(A_1,...,A_L), H_{pq} \in 2^\Theta \tag{2.16}$$

Sub-step 4.2: Construct the belief intervals for identified scenarios

After identifying scenarios by combining beliefs in CCA matrix relations, Bel, Pls and the belief intervals of evaluation grades for identified scenarios are determined by applying Eq. 2.2 and Eq. 2.3 as:

$$\mathrm{Bel}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)) = \sum_{H_{pq} \subseteq H_{pp}} m(H_{pq} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)),\ p,q = 1,...,N \qquad \textbf{(2.17)}$$

$$\mathrm{Pls}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)) = \sum_{H_{pq} \cap H_{pp} \neq \varnothing} m(H_{pq} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)),\ p,q = 1,...,N \qquad \textbf{(2.18)}$$

$$S_t^{'}(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)=\{(H_{pp},[Bel_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)), Pls_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L))]),\ p=1,...,N\} \qquad \textbf{(2.19)}$$

The result is used as a belief interval indicating how strongly the evidence support each scenario. The end points of the belief interval $[\mathrm{Bel}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)), \mathrm{Pls}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L))]$ can be viewed as the lower and upper bounds of the probability to which H_{pp} is supported under the current evidence for scenario $(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)$. Figure 2.2 illustrates the interpretation of the belief interval.

For example;

- If $[\mathrm{Bel}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)), \mathrm{Pls}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L))]$ =[0,0], then there is no evidence to support H_{pp} for scenario $(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)$,
- If $[\mathrm{Bel}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)), \mathrm{Pls}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L))]$ =[0,1], then there is no evidence available either to support or not to support H_{pp} for scenario $(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)$,
- If $[\mathrm{Bel}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)), \mathrm{Pls}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L))]$ =[1,1], H_{pp} for scenario $(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)$ has been completely confirmed,
- If $[\mathrm{Bel}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)), \mathrm{Pls}_t(H_{pp} / T_t(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L))]$ =[0.6,0.9], then the probability of exact support to H_{pp} for scenario $(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)$ is 0.6, and the maximal probability of possible support to H_{pp} for scenario $(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)$ is 0.9, i.e., there is a probability of 0.1 to refuse H_{pp} for scenario $(\mathrm{a}_\cdot^1,...,\mathrm{a}_\cdot^L)$.

Step 5: Evaluate the identified scenarios

In order to evaluate the identified scenarios, the likelihood of identified scenarios is needed to be ranked and compared based on their belief intervals. Therefore, ranking of identified scenarios based on their belief intervals is required.

For this purpose, preference function proposed by Wang is adopted (Wang et al., 2005; Wang et al., 2006). In Wang's method each alternative, here called scenario, has one belief interval. But, because of the different determination of the FD in this study, any scenario could have more than one belief interval; one belief interval for any evaluation grade, H_{pp} (p=1,...,N). Therefore, the degree of preference of scenario A over scenario B for H_{pp} (p=1,...,N) at time t, denoted by $P(A > B, H_{pp})_t \in [0, 1]$, is defined as follows:

$$P(A > B, H_{pp})_t = \frac{\max[0, Pls_t(H_{pp} / A) - Bel_t(H_{pp} / B)] - \max[0, Bel_t(H_{pp} / A) - Pls_t(H_{pp} / B)]}{[Pls_t(H_{pp} / A) - Bel_t(H_{pp} / A)] + [Pls_t(H_{pp} / B) - Bel_t(H_{pp} / B)]} \quad \textbf{(2.20)}$$

According to definition, it is obvious that

- $P(A > B, H_{pp})_t = 1$ if and only if $Bel_t(H_{pp} / A) \geq Pls_t(H_{pp} / B)$,
- $P(A > B, H_{pp})_t = 0$ if and only if $Pls_t(H_{pp} / A) \leq Bel_t(H_{pp} / B)$,
- $P(A > B, H_{pp})_t = 0.5$ if and only if $Bel_t(H_{pp} / A) + Pls_t(H_{pp} / A) = Bel_t(H_{pp} / B) + Pls_t(H_{pp} / A)$,
- $P(A > B, H_{pp})_t > 0.5$ if
  - $Bel_t(H_{pp} / A) > Bel_t(H_{pp} / B)$ and $Pls_t(H_{pp} / A) > Pls_t(H_{pp} / B)$ or
  - $Bel_t(H_{pp} / A) < Bel_t(H_{pp} / B)$, $Pls_t(H_{pp} / A) > Pls_t(H_{pp} / B)$, and $\frac{Bel_t(H_{pp} / A) + Bel_t(H_{pp} / B)}{2} > \frac{Pls_t(H_{pp} / A) + Pls_t(H_{pp} / B)}{2}$.

Therefore, based on above mentioned properties for any evaluation grade, $H_{pp,}$ A is superior to B if $P(A > B, H_{pp})_t > 0.5$, A is indifferent to B if $P(A > B, H_{pp})_t = 0.5$, and A is inferior to B if $P(A > B, H_{pp})_t < 0.5$. The preference function between scenarios has transitivity, i.e., if scenario A is superior to B, and scenario B is

superior to C, then scenario A is superior to C. By applying Eq. 2.20, preference relations among all scenarios can be determined for any evaluation grade, H_{pp}.

In this study, for ranking of scenarios having more than one belief interval, one belief interval for several evaluation grades, new ranking algorithm based on bubble sort is developed. Identified scenarios are sorted from highest likelihood to lowest likelihood according to preference function using bubble sort (Knuth, 1997). Bubble sort is used in this study because bubble sort is one of the simplest sorting algorithms to understand and to implement. Bubble sort works by repeatedly stepping through the list to be sorted, comparing each pair of adjacent items and swapping them if they are in the wrong order. The pass through the list is repeated until no swaps are needed, which indicates that the list is sorted. At the sorting process, there are two alternatives of DM's attitude toward the decision environment: pessimistic or optimistic, in other words risk averse or risk seeking. For the DM's pessimistic attitude, the proposed ranking algorithm is used to identify the worst evaluation grade of any scenario and pick a scenario that has the best of the worst evaluation grade interval based on the preference function mentioned above. For the DM's optimistic attitude, the proposed ranking algorithm is used to select scenario with the best of the best intervals. If one scenario has a higher (or more preferable) evaluation grade value than any of the other scenarios, that scenario is chosen and the sorting process ends. However, if some scenarios are tied on the most important evaluation grade, the subset of tied scenarios is then compared on the next most important evaluation grade. The process continues sequentially until all the alternatives are sorted. Pseudo code implementation of the two proposed ranking algorithm called BubbleSortByMinLikelihood and BubbleSortByMaxLikelihood can be expressed as:

```
procedure BubbleSortByMinLikelihood
( T : list of scenarios )
  do
    swapped = false
    for i = 1 to length(T)-1
      if is_superior (T[i-1],T[i]) then
        swap( T[i-1], T[i] )
        swapped = true
      end if
    end for
  while swapped
end procedure

function is_superior( A,B : scenario )
  for p=1 to N
    if P(A,B,p)> 0.5 then
      return is_superior = false
    end if
  end for
  return is_superior = true
end function
```

```
procedure BubbleSortByMaxLikelihood
( T : list of scenarios )
  do
    swapped = false
    for i = 1 to length(T)-1
      if is_superior (T[i-1],T[i]) then
        swap( T[i-1], T[i] )
        swapped = true
      end if
    end for
  while swapped
end procedure

function is_superior( A,B : scenario )
  for p=N down to 1
    if P(A,B,p)> 0.5 then
      return is_superior = true
    end if
  end for
  return is_superior = false
end function
```

The detailed descriptions of each step are elaborated in the following illustrative case study section.

2.4 An Illustrative Example for Threat Assessment

In this section, the proposed EMA model as described in Section 2.3 is applied to a hypothetical Airport X to identify the threat scenarios and evaluate their likelihoods. Modern airports with their runways, taxiways, aprons, passenger terminals, ground handling and flight navigation equipment are very complex facilities (Ashford, 1997). Simply, the mission of an airport is to land, to unload payload, to load payload and to take off aircrafts. When the security requirements are considered against the possible malevolent attacks, the challenge of threat assessment for an airport becomes very complicated. Therefore, it is thought that an airport case can be an interesting example. Note that for security reasons, all the data used throughout this example are purely generic and notional. Even though this case study is very simple, the resulting qualitative relationships and insights drawn from this example validate the proposed approach.

Assume that at time t officials issued an intelligence bulletin to warn security departments of critical facilities that says “terrorists could target large crowds at holiday gatherings and they might have entered the city with explosive loaded car” and as a security manager of Airport X “what should I do to accomplish a realistic threat assessment?” A step-by-step algorithm for this example is as follows:

Step 1: Identify the parameters and define a range of values for each parameter

In this step, the parameters of the threat scenario are identified and range of values for each parameter is defined for critical facility, Airport X. History of attacks against similar assets and possible methods of attacks are examined. Many of these attacks to date are one-time strike and run-away events. As the attack strategy, attacking a single target is considered, attacking multiple targets is not considered. After data of attacks were collected and compiled for this research from unclassified resources, four critical most common parameters of possible threat scenarios are determined as:

A= {Target (A_1), Weapon type (A_2), Part of target attacked (A_3), Magnitude (A_4)}

Originally more parameters could be defined but this study considers four parameters for possible threat scenarios against critical facility assets. Based on available data and expert knowledge, the detailed descriptions of these parameters and their values are listed below:

- Target (A_1): Targets are specific high value assets at the critical facility, Airport X. After investigating Airport X, 20 possible targets are determined (Ashford, 1997; Akgun et al., 2010).

  A_1 = {"Airfield Maintenance Building" (a_1^1), "Fuel Complex Building" (a_2^1), "Passenger Terminal" (a_3^1), "Parking Facility" (a_4^1), "Bus Station" (a_5^1), "Custom Building" (a_6^1), "Cargo Terminal" (a_7^1), "Air Traffic Control Tower" (a_8^1), "Apron" (a_9^1), "Runway and Taxiway" (a_{10}^1), "Main Entrance and Security Control Building" (a_{11}^1), "Security Building" (a_{12}^1), "Aircraft Rescue and Fire Fighting Building" (a_{13}^1), "Police Station Building" (a_{14}^1), "Fuel Complex Guard Building" (a_{15}^1), "Guard Tower" (a_{16}^1), "Fencing" (a_{17}^1), "Heating Centre Building" (a_{18}^1), "Power Centre Building" (a_{19}^1), "Water Storage Building" (a_{20}^1)}

- Weapon type (A_2): Possible types of the weapon or equipment used for the attacks are determined (Table 2.4). Explosive attacks are most common in historical analysis of past attacks (LaTourrette et al., 2006). In this study, chemical, biological, radiological and nuclear threats are not considered. following weapon types used in disruptive attacks are interested:

  A_2 = {"Explosives" (a_1^2), "Truck/Car bomb" (a_2^2), "Fire/fire bomb" (a_3^2), "Firearms" (a_4^2)}

Table 2.4: Frequency by weapon type of adversary attacks 1998-2005.

Weapon Type	All incidents	
	Number	Percentage (%)
Explosives (nonsuicide and suicide)	6,538	51
Truck/Car bomb (nonsuicide and suicide)	221	1.7
Fire/fire bomb	1,378	10.7
Firearms	3,222	25.1
Knives and sharp objects	175	1.4
Chemical/Biological agent	41	0.3
Other\Unknown	1,256	9.8

- Part of target attacked (A_3): Different part of the target may be subject to attack. Part of the targets subject to attack is classified as:

  A_3={"Perimeter" (a_1^3), "Protected areas" (a_2^3), "Infrastructure Systems" (a_3^3)}

  Perimeter is the peripheral/outside part, protected areas are inside part and infrastructure systems are especially equipment dense part of the targets.
- Magnitude (A_4): Intensity of the attack may vary. Intensity of attacks are categorized as:

  A_4 = {"Low" (a_1^4), "Medium" (a_2^4), "High" (a_3^4)}

Therefore, threat scenario of Airport X is defined as a combination of four parameters: target, weapon type, part of target attacked and magnitude.

Step 2: Form Morphological Field

The morphological field is constructed depending on the information provided by step 1 (Table 2.5). There are totally 20*4*3*3 = 720 threat scenarios either possible or not in the formed morphological field. For example, a threat scenario is developed by the highlighted parameter values that describe a low magnitude explosive attack to perimeter of power centre building in the morphological field (Table 2.5).

Step 3: Construct Cross-Consistency Assessment (CCA) matrix

Sub-step 3.1: Determine the Frame of Discernment for evaluation of CCA matrix relations

Uncertain subjective judgments for evaluation of CCA matrix relation likelihoods are acquired using statements similar to statements 1-5. It is important to capture fine threat likelihood distinction among threat scenarios with proposed linguistic evaluation grades that represent the input information. In this study, security experts give their subjective judgements linguistically by means of a following mutually exclusive set of evaluation grades: "Likely" (L), "Very Likely" (VL), "Highly Likely" (HL), "Very Highly Likely" (VHL) and "Extremely Likely" (EL). In the terminology of DST, the FD, Θ, is defined as follows:

$$\Theta = \{\mathrm{L}, \mathrm{VL}, \mathrm{HL}, \mathrm{VHL}, \mathrm{EL}\} = \{H_{11}, H_{22}, H_{33}, H_{44}, H_{55}\} \quad \textbf{(2.21)}$$

Therefore, all of the relations between each scenario parameter are assessed on the basis of individual evaluation grades H_{pq} (p=q,p=1,…,5) and the interval evaluation grades between H_{pp} and H_{qq} (p<q,q=2,…,5) similar to statements 1-5 as:

$$\begin{Bmatrix} L & L-VL & L-HL & L-VHL & L-EL \\ & VL & VL-HL & VL-VHL & VL-EL \\ & & HL & HL-VHL & HL-EL \\ & & & VHL & VHL-EL \\ & & & & EL \end{Bmatrix} = \begin{Bmatrix} H_{11} & H_{12} & H_{13} & H_{14} & H_{15} \\ & H_{22} & H_{23} & H_{24} & H_{25} \\ & & H_{33} & H_{34} & H_{35} \\ & & & H_{44} & H_{45} \\ & & & & H_{55} \end{Bmatrix}$$

(2.22)

Table 2.5: Morphological field of the case study.

Target (A_1)	Weapon Type(A_2)	Part of Target Attacked (A_3)	Magnitude (A_4)
a_1^1 Airfield Maintenance Building	a_1^2 Explosives	a_1^3 Perimeter	a_1^4 Low
a_2^1 Fuel Complex Building	a_2^2 Truck/Car bomb	a_2^3 Protected areas	a_2^4 Medium
a_3^1 Passenger Terminal	a_3^2 Fire/Fire bomb	a_3^3 Infrastructure systems	a_3^4 High
a_4^1 Parking Facility	a_4^2 Firearms		
a_5^1 Bus Station			
a_6^1 Custom Building			
a_7^1 Cargo Terminal			
a_8^1 Air Traffic Control Tower			
a_9^1 Apron			
a_{10}^1 Runway and Taxiway			
a_{11}^1 Main Entrance and Security Control Building			
a_{12}^1 Security Building			
a_{13}^1 Aircraft Rescue & Fire Fighting Building			
a_{14}^1 Police Station Building			
a_{15}^1 Fuel Complex Guard Building			
a_{16}^1 Guard Tower			
a_{17}^1 Fencing			
a_{18}^1 Heating Centre Building			
a_{19}^1 Power Centre Building			
a_{20}^1 Water Storage Building			

Sub-step 3.2: Assign bpas for evaluation grades of CCA matrix relations

In the proposed model, the relations among threat scenario parameters in CCA are required to be evaluated. All the evidence of a threat will be in the form of intelligence information and analyses of past adversary attacks. Reliable threat data are the most difficult to assess because prediction of adversary intentions are complex and difficult. Although historical data can help to define threat likelihood, it must be interpreted by considering technical capabilities of attacker, the attacker's perception of both the vulnerability and the potential consequences from a successful attack of the target. Attacker will attack the targets with high consequence and high vulnerable in order to maximize expected consequence. The attacker's intelligence/knowledge of the system may vary. The attacker may have perfect intelligence, partial intelligence, bad intelligence or no intelligence. Perception and capabilities of attackers are also not known. Therefore, identifying all of the actions into the future is not possible.

The experts (intelligence, weapons, weapon delivery systems, etc.) and their knowledge base examining the current evidence become the basis for assigning bpas to evaluation grades of CCA matrix relations. The experts typically ask the question, "If I were an attacker, I would ..." thinking like an attacker and assign bpas to simple relations in CCA rather than complex relations without getting overloaded considering above mentioned facts. The use of judgment is necessary because of the subjective nature of these assessments and the experts can cast this information into an easy form provided by proposed EMA model.

In this study, the evidence is quantified by representing it as a belief structures that clearly communicates the uncertainty based on the quality of the evidence. The belief structures are easy to use and very flexible way to expert judgements and can help to better evaluate the threat likelihood. In terms of the defined evaluation grades, experts express their opinions using belief structure and providing consensus evaluation for each relation. Each relation is described by evaluation grades and their associated bpas. Explicitly, the assigned bpas represents the degree of expert belief for each evaluation grade, and implicitly, it represents the total evidence to clarify the threat scenario likelihood.

By using expert judgement, the belief structure of any relation based on intelligence at time t reporting "possible bomb attack especially focusing on civilians" is given in

Table 2.6. For example, in Table 2.6 the belief structure of $(a_3^1, a_1^2) \in R_{12}^t(a_k^1, a_l^2)$ at time t is $S_t(a_3^1, a_1^2) = \{(H_{11}, 0.4), (H_{25}, 0.2)\}$.

Step 4: Synthesize an internally consistent outcome space

Sub-step 4.1: Combine beliefs in CCA matrix relations

In this case study, the morphological field is defined by four basic parameters. Therefore, there are six (C_2^4) relations in CCA matrix, and the information collected by experts comes from these six different relations that constructs a threat scenario. These relations are independent pieces of evidence offering information on the experts' knowledge towards the likelihood of the threat scenario. Threat scenarios are constructed depending on evaluation grades of each relation using the DP's rule (Eq. 2.5) and the Yager's rule (Eq. 2.6) as follows:

$$\begin{aligned} m_t(H_{pq} / T(a_\cdot^1, a_\cdot^2, a_\cdot^3, a_\cdot^4)) = \sum m_t(H_{pq} / R_{12}(a_\cdot^1, a_\cdot^2)) \oplus m_t(H_{pq} / R_{13}(a_\cdot^1, a_\cdot^3)) \\ \oplus m_t(H_{pq} / R_{14}(a_\cdot^1, a_\cdot^4)) \oplus m_t(H_{pq} / R_{23}(a_\cdot^2, a_\cdot^3)) \\ \oplus m_t(H_{pq} / R_{24}(a_\cdot^2, a_\cdot^4)) \oplus m_t(H_{pq} / R_{34}(a_\cdot^3, a_\cdot^4)) \end{aligned} \quad \textbf{(2.23)}$$

Sample combination of two relations by using both rules is shown in Table 2.7 and Table 2.8.

Table 2.6: CCA matrix at time t.

		Weapon Type		Part of target attacked		Magnitude	
		a_1^2	a_2^2	a_1^3	a_2^3	a_1^4	a_2^4
Target	a_3^1	$\{(H_{11},0.4),(H_{25},0.2)\}^*$	-	$\{(H_{34},0.7),(H_{55},0.3)\}$	$\{(H_{12},0.6),(H_{34},0.2)\}^*$	$\{(H_{34},0.5),(H_{55},0.5)\}$	$\{(H_{12},0.6),(H_{34},0.4)\}$
	a_4^1	-	$\{(H_{12},0.5),(H_{34},0.2)\}^*$	-	$\{(H_{34},0.4),(H_{55},0.6)\}$	$\{(H_{13},0.7),(H_{45},0.3)\}$	$\{(H_{34},0.8),(H_{55},0.2)\}$
	a_5^1	$\{(H_{12},0.6),(H_{35},0.4)\}$	-	$\{(H_{33},0.2),(H_{45},0.8)\}$	$\{(H_{13},0.5),(H_{44},0.5)\}$	$\{(H_{12},0.6),(H_{35},0.4)\}$	$\{(H_{12},0.5),(H_{33},0.4)\}^*$
	a_{11}^1	$\{(H_{12},0.4),(H_{33},0.3)\}^*$	-	$\{(H_{13},0.7),(H_{45},0.3)\}$	-	$\{(H_{13},0.6),(H_{45},0.4)\}$	$\{(H_{33},0.7),(H_{45},0.3)\}$
Weapon Type	a_1^2			$\{(H_{22},0.2),(H_{35},0.8)\}$	$\{(H_{13},0.7),(H_{45},0.3)\}$	$\{(H_{33},0.6),(H_{45},0.3)\}^*$	$\{(H_{22},0.5)\}^*$
	a_2^2			$\{(H_{33},0.3),(H_{45},0.7)\}$	$\{(H_{22},0.4),(H_{35},0.5)\}^*$	$\{(H_{12},0.4),(H_{34},0.6)\}$	$\{(H_{12},0.5),(H_{34},0.5)\}$
Part of target attacked	a_1^3					$\{(H_{12},0.6),(H_{35},0.4)\}$	$\{(H_{13},0.7),(H_{45},0.3)\}$
	a_2^3					$\{(H_{12},0.7),(H_{33},0.3)\}$	$\{(H_{11},0.8),(H_{23},0.2)\}$

note: "*" refers to incomplete information.

Table 2.7: Combination of $R_{12}^{t}(a_3^1, a_1^2)$ and $R_{13}^{t}(a_3^1, a_1^3)$ by DP's rule.

$R_{12}^{t}(a_3^1, a_1^2) \oplus R_{13}^{t}(a_3^1, a_1^3)$			$R_{13}^{t}(a_3^1, a_1^3)$			
			Interval	m_t	Interval	m_t
			H_{34}	0.7	H_{55}	0.3
$R_{12}^{t}(a_3^1, a_1^2)$	Interval	m_t				
	H_{11}	0.4	$[H_{11}, H_{34}]$	0.28	$[H_{11}, H_{55}]$	0.12
	H_{25}	0.2	H_{25}	0.14	H_{25}	0.06
	Θ	0.4	Θ	0.28	Θ	0.12
$\sum_{B_i \cup B_j = A} m_1(B_i) m_2(B_j)$	{([H_{11},H_{34}], 0.28), ([H_{11},H_{55}], 0.12), (H_{25}, 0.2)}					
$m_1 \oplus_{DP} m_2(A)$	{([H_{11},H_{34}], 0.28), ([H_{11},H_{55}], 0.12), (H_{25}, 0.2), (Θ, 0.4)}					

Note that if there is an intersection, the union of two intervals in Table 2.7 is defined by the set consisting minimum of the two lower bounds and the maximum of the two upper bounds corresponding to an intersection. If there is no intersection, the union of two intervals in Table 2.7 is defined by the set consisting of two intervals separately.

Table 2.8: Combination of $R_{12}^{t}(a_3^1, a_1^2)$ and $R_{13}^{t}(a_3^1, a_1^3)$ by Yager's rule.

$R_{12}^{t}(a_3^1, a_1^2) \oplus R_{13}^{t}(a_3^1, a_1^3)$			$R_{13}^{t}(a_3^1, a_1^3)$			
			Interval	m_t	Interval	m_t
			H_{34}	0.7	H_{55}	0.3
$R_{12}^{t}(a_3^1, a_1^2)$	Interval	m_t				
	H_{11}	0.4	Ø	0.28	Ø	0.12
	H_{25}	0.2	H_{34}	0.14	H_{55}	0.06
	Θ	0.4	H_{34}	0.28	H_{55}	0.12
K	0.4					
$\sum_{B_i \cap B_j = A} m_1(B_i) m_2(B_j)$	{(H_{34}, 0.42), (H_{55}, 0.18)}					
$m_1 \oplus_{Yager} m_2(A)$	{(H_{34}, 0.42), (H_{55},0.18), (Θ, 0.4)}					

Note that the intersection of two intervals in Table 2.8 is defined by the maximum of the two lower bounds and the minimum of the two upper bounds corresponding to an intersection. For K, there are two cells that contribute to conflict represented by empty intersections and using Eq. 2.7, K= (0.4*0.7)+(0.4*0.3)=0.4.

Belief structures of identified threat scenarios at time t by using both combination rules is shown in Table 2.9.

Table 2.9: Belief structures of identified threat scenarios.

Rule	No.	$S_t(.)$	Belief Structure
DP	1	$S_t(a_3^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{14}, 0.0101), (H_{25}, 0.0720), (\Theta, 0.9179)\}$
	2	$S_t(a_3^1, a_1^2, a_2^3, a_1^4)$	$\{(H_{14}, 0.0672), (H_{25}, 0.0032), (\Theta, 0.9296)\}$
	3	$S_t(a_3^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{14}, 0.0196), (H_{25}, 0.0120), (\Theta, 0.9684)\}$
	4	$S_t(a_3^1, a_1^2, a_2^3, a_2^4)$	$\{(H_{12}, 0.0230), (H_{13}, 0.0058), (H_{14}, 0.0992), (H_{25}, 0.0014), (\Theta, 0.8706)\}$
	5	$S_t(a_4^1, a_2^2, a_2^3, a_1^4)$	$\{(H_{14}, 0.0784), (H_{25}, 0.0043), (H_{35}, 0.0054), (\Theta, 0.9119)\}$
	6	$S_t(a_4^1, a_2^2, a_2^3, a_2^4)$	$\{(H_{14}, 0.0870), (H_{24}, 0.0026), (H_{25}, 0.0154), (\Theta, 0.8950)\}$
	7	$S_t(a_5^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{13}, 0.0052), (H_{25}, 0.0115), (H_{35}, 0.0461), (\Theta, 0.9372)\}$
	8	$S_t(a_5^1, a_1^2, a_2^3, a_1^4)$	$\{(H_{13}, 0.0756), (H_{14}, 0.0756), (H_{35}, 0.0065), (\Theta, 0.8423)\}$
	9	$S_t(a_5^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{13}, 0.0076), (H_{25}, 0.0240), (\Theta, 0.9684)\}$
	10	$S_t(a_5^1, a_1^2, a_2^3, a_2^4)$	$\{(H_{13}, 0.0945), (H_{14}, 0.0945), (H_{25}, 0.0024), (\Theta, 0.8086)\}$
	11	$S_t(a_{11}^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{13}, 0.0212), (H_{25}, 0.0026), (H_{35}, 0.0104), (\Theta, 0.9659)\}$
	12	$S_t(a_{11}^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{13}, 0.0240), (H_{25}, 0.0135), (\Theta, 0.9625)\}$
Yager	1	$S_t(a_3^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{33}, 0.0269), (H_{34}, 0.0022), (H_{44}, 0.0134), (H_{55}, 0.0131), (\Theta, 0.9444)\}$
	2	$S_t(a_3^1, a_1^2, a_2^3, a_1^4)$	$\{(H_{33}, 0.0149), (\Theta, 0.9851)\}$
	3	$S_t(a_3^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{33}, 0.0470), (H_{44}, 0.0202), (\Theta, 0.9328)\}$
	4	$S_t(a_3^1, a_1^2, a_2^3, a_2^4)$	$\{(H_{11}, 0.0077), (H_{22}, 0.0137), (H_{33}, 0.0058), (\Theta, 0.9729)\}$
	5	$S_t(a_4^1, a_2^2, a_2^3, a_1^4)$	$\{(H_{33}, 0.0126), (\Theta, 0.9874)\}$
	6	$S_t(a_4^1, a_2^2, a_2^3, a_2^4)$	$\{(H_{33}, 0.0096), (\Theta, 0.9904)\}$
	7	$S_t(a_5^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{33}, 0.0061), (H_{45}, 0.0123), (\Theta, 0.9816)\}$
	8	$S_t(a_5^1, a_1^2, a_2^3, a_1^4)$	$\{(H_{12}, 0.0088), (H_{33}, 0.0118), (\Theta, 0.9764)\}$
	9	$S_t(a_5^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{33}, 0.0090), (H_{45}, 0.0038), (\Theta, 0.9872)\}$
	10	$S_t(a_5^1, a_1^2, a_2^3, a_2^4)$	$\{(H_{11}, 0.0504), (H_{22}, 0.0273), (H_{33}, 0.0070), (\Theta, 0.9153)\}$
	11	$S_t(a_{11}^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{22}, 0.0035), (H_{33}, 0.0564), (H_{45}, 0.0046), (\Theta, 0.9354)\}$
	12	$S_t(a_{11}^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{33}, 0.0412), (H_{45}, 0.0032), (\Theta, 0.9556)\}$

Sub-step 4.2: Construct the belief intervals for identified scenarios

After identifying threat scenarios by combining beliefs in CCA matrix relations, Bel, Pls and the belief intervals of evaluation grades for identified threat scenarios are determined by applying Eq. 2.2 and Eq. 2.3 as:

$$\mathrm{Bel}_t(H_{pp} / T_t(a_\cdot^1, a_\cdot^2, a_\cdot^3, a_\cdot^4)) = \sum_{H_{pq} \subseteq H_{pp}} m(H_{pq} / T_t(a_\cdot^1, a_\cdot^2, a_\cdot^3, a_\cdot^4)),\ p, q = 1, ..., 5 \qquad \textbf{(2.24)}$$

$$\mathrm{Pls}_t(H_{pp} / T_t(\mathrm{a}_{\cdot}^1, \mathrm{a}_{\cdot}^2, \mathrm{a}_{\cdot}^3, \mathrm{a}_{\cdot}^4)) = \sum_{H_{pq} \cap H_{pp} \neq \varnothing} m(H_{pq} / T_t(\mathrm{a}_{\cdot}^1, \mathrm{a}_{\cdot}^2, \mathrm{a}_{\cdot}^3, \mathrm{a}_{\cdot}^4)),\ p, q = 1, ..., 5 \qquad \textbf{(2.25)}$$

$$\mathrm{S}_t^{'}(\mathrm{a}_{\cdot}^1, \mathrm{a}_{\cdot}^2, \mathrm{a}_{\cdot}^3, \mathrm{a}_{\cdot}^4) = \left\{(H_{pp}, [\mathrm{Bel}_t(H_{pp} / T_t(\mathrm{a}_{\cdot}^1, \mathrm{a}_{\cdot}^2, \mathrm{a}_{\cdot}^3, \mathrm{a}_{\cdot}^4)), \mathrm{Pls}_t(H_{pp} / T_t(\mathrm{a}_{\cdot}^1, \mathrm{a}_{\cdot}^2, \mathrm{a}_{\cdot}^3, \mathrm{a}_{\cdot}^4))]),\ p = 1, ..., 5\right\} \qquad \textbf{(2.26)}$$

The belief intervals calculated for the identified threat scenarios by using both combination rules are provided in Table 2.10 and plotted in Figure 2.4 and Figure 2.5.

Table 2.10: Belief intervals for threat scenarios.

Rule	No	Threat Scenario	H_{11}		H_{22}		H_{33}		H_{44}		H_{55}	
			Bel	Pls	Bel	Pls	Bel	Pls	Bel	Pls	Bel	Pls
DP	1	$\mathrm{S}_t'(\mathrm{a}_3^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_1^4)$	0	0.9280	0	1	0	1	0	1	0	0.9899
	2	$\mathrm{S}_t'(\mathrm{a}_3^1, \mathrm{a}_1^2, \mathrm{a}_2^3, \mathrm{a}_1^4)$	0	0.9968	0	1	0	1	0	1	0	0.9328
	3	$\mathrm{S}_t'(\mathrm{a}_3^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_2^4)$	0	0.9880	0	1	0	1	0	1	0	0.9804
	4	$\mathrm{S}_t'(\mathrm{a}_3^1, \mathrm{a}_1^2, \mathrm{a}_2^3, \mathrm{a}_2^4)$	0	0.9986	0	1	0	0.9770	0	0.9712	0	0.8720
	5	$\mathrm{S}_t'(\mathrm{a}_4^1, \mathrm{a}_2^2, \mathrm{a}_2^3, \mathrm{a}_1^4)$	0	0.9903	0	0.9946	0	1	0	1	0	0.9216
	6	$\mathrm{S}_t'(\mathrm{a}_4^1, \mathrm{a}_2^2, \mathrm{a}_2^3, \mathrm{a}_2^4)$	0	0.9820	0	1	0	1	0	1	0	0.9104
	7	$\mathrm{S}_t'(\mathrm{a}_5^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_1^4)$	0	0.9424	0	0.9539	0	1	0	0.9948	0	0.9948
	8	$\mathrm{S}_t'(\mathrm{a}_5^1, \mathrm{a}_1^2, \mathrm{a}_2^3, \mathrm{a}_1^4)$	0	0.9935	0	0.9935	0	1	0	0.9244	0	0.8488
	9	$\mathrm{S}_t'(\mathrm{a}_5^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_2^4)$	0	0.9760	0	1	0	1	0	0.9924	0	0.9924
	10	$\mathrm{S}_t'(\mathrm{a}_5^1, \mathrm{a}_1^2, \mathrm{a}_2^3, \mathrm{a}_2^4)$	0	0.9976	0	1	0	1	0	0.9055	0	0.8110
	11	$\mathrm{S}_t'(\mathrm{a}_{11}^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_1^4)$	0	0.9870	0	0.9896	0	1	0	0.9788	0	0.9788
	12	$\mathrm{S}_t'(\mathrm{a}_{11}^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_2^4)$	0	0.9865	0	1	0	1	0	0.9760	0	0.9760
Yager	1	$\mathrm{S}_t'(\mathrm{a}_3^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_1^4)$	-	-	-	-	0.0269	0.9734	0.0134	0.9600	0.0131	0.9574
	2	$\mathrm{S}_t'(\mathrm{a}_3^1, \mathrm{a}_1^2, \mathrm{a}_2^3, \mathrm{a}_1^4)$	-	-	-	-	0.0149	1	-	-	-	-
	3	$\mathrm{S}_t'(\mathrm{a}_3^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_2^4)$	-	-	-	-	0.0470	0.9798	0.0202	0.9530	-	-
	4	$\mathrm{S}_t'(\mathrm{a}_3^1, \mathrm{a}_1^2, \mathrm{a}_2^3, \mathrm{a}_2^4)$	0.0077	0.9806	0.0137	0.9866	0.0058	0.9786	-	-	-	-
	5	$\mathrm{S}_t'(\mathrm{a}_4^1, \mathrm{a}_2^2, \mathrm{a}_2^3, \mathrm{a}_1^4)$	-	-	-	-	0.0126	1	-	-	-	-
	6	$\mathrm{S}_t'(\mathrm{a}_4^1, \mathrm{a}_2^2, \mathrm{a}_2^3, \mathrm{a}_2^4)$	-	-	-	-	0.0096	1	-	-	-	-
	7	$\mathrm{S}_t'(\mathrm{a}_5^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_1^4)$	-	-	-	-	0.0061	0.9877	0	0.9939	0	0.9939
	8	$\mathrm{S}_t'(\mathrm{a}_5^1, \mathrm{a}_1^2, \mathrm{a}_2^3, \mathrm{a}_1^4)$	0	0.9882	0	0.9882	0.0118	0.9912	-	-	-	-
	9	$\mathrm{S}_t'(\mathrm{a}_5^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_2^4)$	-	-	-	-	0.0090	0.9962	0	0.9910	0	0.9910
	10	$\mathrm{S}_t'(\mathrm{a}_5^1, \mathrm{a}_1^2, \mathrm{a}_2^3, \mathrm{a}_2^4)$	0.0504	0.9657	0.0273	0.9426	0.0070	0.9223	-	-	-	-
	11	$\mathrm{S}_t'(\mathrm{a}_{11}^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_1^4)$	-	-	0.0035	0.9389	0.0564	0.9919	0	0.9400	0	0.9400
	12	$\mathrm{S}_t'(\mathrm{a}_{11}^1, \mathrm{a}_1^2, \mathrm{a}_1^3, \mathrm{a}_2^4)$	-	-	-	-	0.0412	0.9968	0	0.9588	0	0.9588

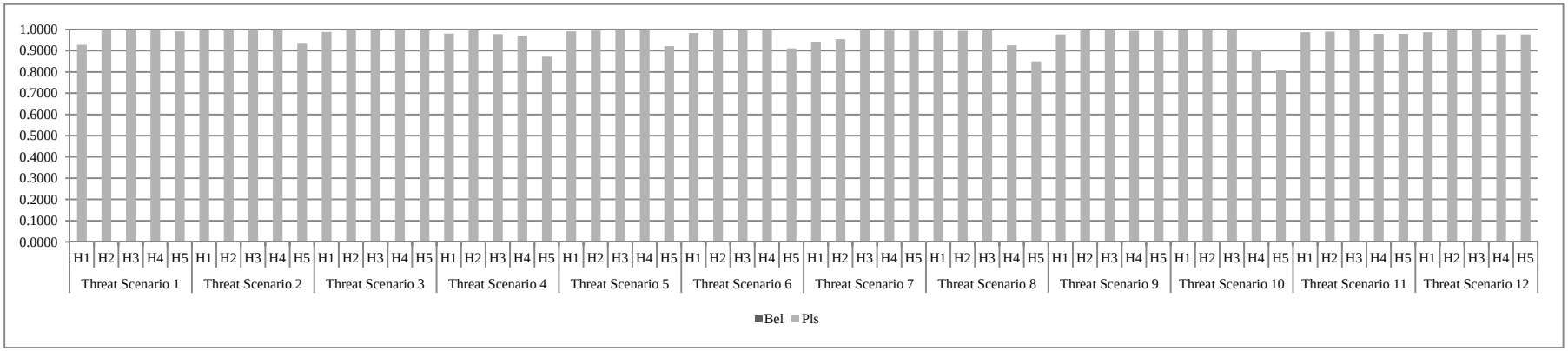


Figure 2.4 : The belief intervals of DP's rule.

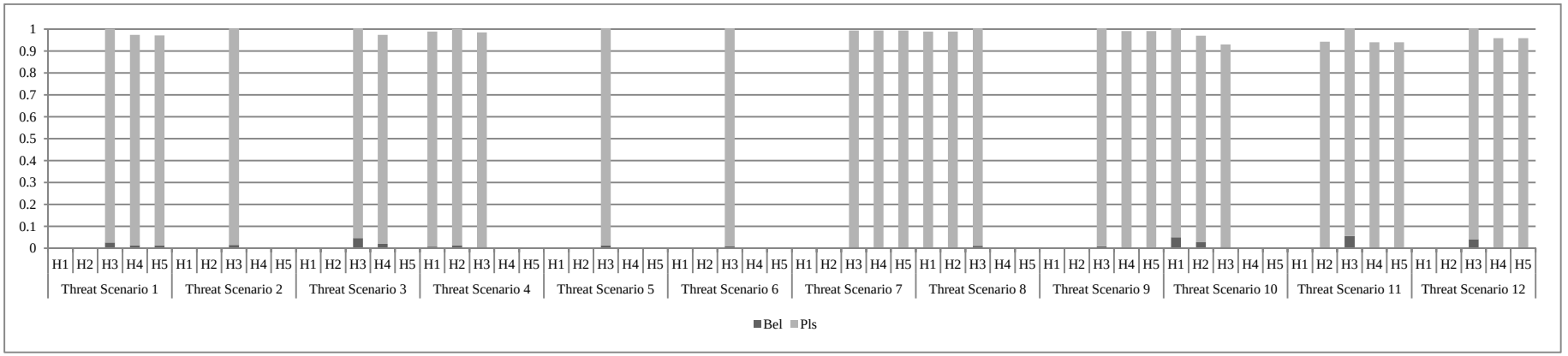


Figure 2.5 : The belief intervals of Yager's rule.

When the two rules are compared, the Yager's rule transfers the conflict into the total ignorance by adding K to joint evidence of Θ but the DP's rule does not generate any conflict. In other words, the Yager's rule as conjunctive rule (AND-based on set intersection) discards the conflict information and increases the total ignorance but the DP's rule as a disjunctive rule (OR-based on set union) does not reject any information asserted by the sources. It is seen that the DP's rule provides larger belief intervals to more evaluation grades for the same threat scenarios than the Yager's rule. Therefore, when the conflict is higher (for a higher K value), the total ignorance will increase significantly and the Yager's rule gives more stable and robust results than the DP's rule. The drawback of DP's rule is that it yields more imprecise result than desirable when there is a strong conflict among relations.

Step 5 : Evaluate the identified scenarios

At this step, the likelihood of identified scenarios are ranked and compared based on their belief intervals by the developed sorting algorithm. The results are interpreted to guide threat assessment. The ranking of 12 identified threat scenarios based on their likelihoods is calculated and presented in Table 2.11. Since there are two DST combination rules and two sorting algorithms, four ranking alternatives are presented in Table 2.11. Rankings enable the DMs to identify the higher likelihood scenarios from the lower likelihood ones.

Risk bearer's attitude, either risk seeking or risk averse, is important when choosing the approporiate ranking among four different ranking alternatives. For risk seeking attitude, ranking based on Yager's rule with sorting algorithm by maximum likelihood is appropriate and for risk averse attitude, ranking based on DP's rule with sorting algorithm by minimum likelihood is appropriate. As risk bearer's attitude is subjective, it is assumed that risk bearer is rational and aware of this issue.

After threat assessment has been completed based on the intelligence at time t, depending on the ranking of security risks from highest likelihood to lowest likelihood, security risk management can be accomplished by allocating available security risk management resources to security risk-reducing countermeasures (e.g., for vulnerability reduction or consequence mitigation) from the top of the list down. Fine threat likelihood distinction among threat scenarios can be captured with proposed EMA model that represents the available input information. Therefore,

EMA model can be used to reason about threat likelihood and provide adequate precision for threat assessment.

Table 2.11: Threat scenario rankings based on belief intervals.

No.	Threat Scenario	Ranking			
		DP		Yager	
		By Min Likelihood	By Max Likelihood	By Min Likelihood	By Max Likelihood
1	$(a_3^1, a_1^2, a_1^3, a_1^4)$	**1**	3	2	3
2	$(a_3^1, a_1^2, a_2^3, a_1^4)$	10	7	6	7
3	$(a_3^1, a_1^2, a_1^3, a_2^4)$	7	4	7	6
4	$(a_3^1, a_1^2, a_2^3, a_2^4)$	**12**	10	10	11
5	$(a_4^1, a_2^2, a_2^3, a_1^4)$	8	8	5	8
6	$(a_4^1, a_2^2, a_2^3, a_2^4)$	4	9	4	9
7	$(a_5^1, a_1^2, a_1^3, a_1^4)$	2	**1**	**1**	**1**
8	$(a_5^1, a_1^2, a_2^3, a_1^4)$	9	11	11	10
9	$(a_5^1, a_1^2, a_1^3, a_2^4)$	3	2	3	2
10	$(a_5^1, a_1^2, a_2^3, a_2^4)$	11	**12**	**12**	**12**
11	$(a_{11}^1, a_1^2, a_1^3, a_1^4)$	6	5	9	5
12	$(a_{11}^1, a_1^2, a_1^3, a_2^4)$	5	6	8	4

2.5 Concluding Remarks of Chapter 2

In SRA, there is a need for understanding the threats involved. Therefore, the main goal of this study is to identify threats for which there is intelligence of an imminent threat and estimate their likelihoods for critical facility protection. For this purpose, a novel approach called Evidence based Morphological Analysis (EMA) is proposed by describing reasons for modelling uncertainty by DST, the fundamentals of DST and MA, and how DST is applied for threat likelihood estimation within MA.

Firstly, the appropriate uncertainty model for threat assessment of a critical facility is discussed in detail by considering the type of input information at hand, the quality of required output information, and the axiomatic assumptions about the cause of uncertainty. It is stated that DST is the appropriate uncertainty model for threat likelihood estimation since threat is neither random event nor vague event and uncertainty associated with such intelligent event involves epistemic uncertainty.

Secondly, qualitative method MA is integrated with DST. Original FD is determined for evaluation of relations considering computational complexity. Determination of the FD for input data is the most informative and is the efficient way of capturing and quantifying the state of knowledge about the likelihood of a defined threat scenario for a critical facility. The proposed model allows to express qualitative judgements using belief structures developed on the basis of DST and make full use of available information without information loss and exaggeration. EMA also converts limited information to quantifiable threat likelihood parameter for quantitative analysis based on the complete and/or incomplete information which can be both linguistic evaluation grades and interval evaluation grades. The notion of time, t, is also introduced into the problem formulation because a relation in MA may change when more information is get by time.

To summarize, EMA is a quantified MA that integrates MA with DST. The strength of MA provides both identifying and developing the plausible scenarios while DST allows for both the definition and the quantification of relationships between parameters of the scenario in MA. Scenarios are developed by combining simple relations using two most common DST combination rules. The two most common DST combination rules (conjunctive and disconjunctive) are analyzed for threat likelihood estimation by considering DM's attitude (risk averse and risk seeking) and new interval sorting algorithm is developed for scenario ranking. EMA analyzes and handles a wide range of plausible scenarios more easily than hierarchical techniques as tree structures with modest computational effort. By using EMA, alternative threat scenarios can be formulated, developed and evaluated in a structured way. This approach provides required output data precision for comparing and ranking of threat scenarios systematically.

An important feature of EMA is the ability to update easily with less computational burden. The threat is usually assumed to be static but dynamic SRA requires dynamic threat assessment. Intelligent attackers innovate and threat scenarios evolve based on changing conditions as changing defences, technology and social situations in an adaptive way. When new intelligence information about adversary intent and assumed adversary capabilities become available, EMA can be easily updated by recalculating only the affected threat scenario likelihoods or extending the morphological field (adding new parameters or adding new parameter values). Since

likelihood estimation is a continuous process, the new information obtained can be used easily as a feedback for the proposed model to update evaluation.

As a result, EMA has been successfully used to represent the threat likelihood for critical facility by synthesizing linguistic judgement information of experts. This approach better captures the uncertainty in threat assessment than traditional probabilistic risk approaches that use point estimates. EMA improves threat assessment and is shown to be a useful tool in threat assessment of critical facilities in a simple case study. EMA is not limited to threat assessment and can also be applied to likelihood estimation problems involving epistemic uncertainty and scenario development.

3. VULNERABILITY ASSESSMENT MODELLING

3.1 Introduction to Vulnerability Assessment

Critical facility vulnerability assessment is a highly complex strategic activity in security risk assessment (SRA) and necessitates a structured quantified methodology to support the decision making process in defence planning. In the system perspective, the critical facility, such as airport, dam, governmental facility, harbour, nuclear power plant, oil plant etc., can be defined as a system that relies on a group of different interdependent logical and physical entities as system functions and system components.

The aim of this chapter is to present a realistic approach to determine the vulnerability of such a system defended against the adversary attack under multiple criteria which can be both qualitative and quantitative by considering these interdependencies. The proposed approach, called fuzzy integrated vulnerability assessment model (FIVAM), is based on fuzzy set theory, Simple Multi-Attribute Rating Technique (SMART) and Fuzzy Cognitive Maps (FCM) methodology in a group decision-making environment (Akgün et al., 2010). The FIVAM approach is presented step by step and applied to a simple case study on airport vulnerability assessment. The results of the application are compared to those observed through a classical vulnerability assessment model to illustrate the effectiveness of the FIVAM. Furthermore, FIVAM provides a framework to identify the hidden vulnerabilities caused by the functional interdependencies within the system. The results also show that FIVAM quantifies the vulnerability of the system, system functions and system components, and determines the most critical functions and components by simulating the system behaviour.

For SRA, vulnerability assessment of a system defended against adversary attack is initial and crucial step (Garrick et al., 2004; Sarewitz et al., 2003). Vulnerability can be defined as a “weakness in the system defended” in a most common and simplest way. Indeed, more vulnerable means easier to be damaged or harmed. Although a

comprehensive list of vulnerability definitions can be found in Ezell (2007), the term vulnerability still remains as a vague term. Therefore, a workable definition of vulnerability is especially difficult to formulate and quantify. Vulnerability must be quantifiable so that vulnerability assessment before adversary attack occurs can be done. Vulnerability assessment is a systematic process of identification and evaluation of system vulnerabilities (Garrick et al., 2004). Firstly, vulnerability assessment is intended to identify the weaknesses of a system that adversaries can exploit. Then, vulnerabilities that are most significant are evaluated and focused on. It may be impractical or usually even impossible to eliminate all system vulnerabilities because of time and resource constraints. It is required to be aware of these vulnerabilities for developing the necessary defence methods and for assigning the defence resources consistently.

As critical facilities are complex both topologically and functionally, critical facility vulnerability assessment is a challenging issue. As the complexity of a system increases, ability to make precise and yet significant statements about its behaviour diminishes (Zadeh, 1975a;b;c). Each critical facility as a system contains some degree of vulnerability and vulnerabilities may have different effects on the system and its functions/services. System functions are addressed as purposeful actions that system components contribute to accomplish system mission. System functions are not physical entities like system components and the dependence between system functions and system components, physical dependencies, is frequently difficult to assess accurately. In addition to this, system functions are not independent of each other. Because of high degree of uncertainties, it is also difficult to discover quantitative and precise information on system function interdependencies. Interaction among system functions produces the emergence of complex relationships that are not predictable by the knowledge of any single system function. Designing a realistic vulnerability assessment necessitates consideration of complex causal relationships among various system functions, logical dependencies. Both the presence of either hidden or poorly understood interdependencies and their cascading effects are required to be handled. Previous studies on this issue have largely ignored the possible interrelationships among the system functions that affect the system state.

It is extremely difficult in security case to obtain exact data under uncertainty against an adversarial and adaptive opponent. Much of the information related to vulnerability assessment is not quantitative. Rather, this incomplete and imprecise information is expressed qualitatively as words or phrases in a natural language by experts of different fields such as terrorism experts, security experts, engineers, and academicians. Individual opinions, evaluations and ratings from these experts must be identified and applied to vulnerability assessment. Vulnerability assessment problem can be recognized as a group decision-making (GDM) problem under multiple criteria. Therefore, there is a value in considering the fuzzy set theory and GDM methods for critical facility vulnerability assessment.

The purpose of this chapter is to present a fuzzy integrated vulnerability assessment model (FIVAM) based on fuzzy SMART and FCM techniques to assess the vulnerability of a critical facility in the GDM environment. The proposed FIVAM approach enables to determine the vulnerability values under multiple criteria as well as provides a framework to simulate the system vulnerability behaviour depending on the vulnerabilities of the interdependent system functions. Additionally, FIVAM allows the decision makers to identify the hidden vulnerabilities caused by the functional interdependencies within the system.

The remainder of this chapter is organized as follows: Section 3.2 overviews the existing approaches and the factors that influence the system vulnerability assessment. In Section 3.3, fundamentals of fuzzy set theory, the theoretical framework of SMART and the principles of FCM are represented. The proposed FIVAM and its process flow are introduced in Section 3.4. The illustrative application of FIVAM is performed over an airport case study in Section 3.5. This section also examines the utility of findings and discusses the analysis results. Conclusions and further issues are addressed respectively in the final section.

3.2 Literature Review on Vulnerability Assessment

There is confusion in the terms “vulnerability” and “risk” as applied to SRA in the literature. To overcome this issue, Ezell (2007) presented a relationship emerging between vulnerability and risk. According to his study, vulnerability highlights the notion of susceptibility to a scenario, whereas risk focuses on the severity of

consequences within the context of a scenario. In addition to this, Willis (2007) defined security risk as a function of threat, vulnerability and consequences. Vulnerability assessment is generally employed as a sub process of risk assessment in the previous studies (Garrick et al., 2004).

Recently, vulnerability assessment has gained a dynamic and complex nature, and become an active area of research due to its increasing strategic significance in various application areas. However, the focus of this chapter is limited to the researches for critical facility vulnerability assessment in SRA. This survey also incorporates the studies for critical infrastructures vulnerability assessment briefly, as critical facilities rely on these critical infrastructures and have some key critical infrastructure components together with system specific components within their system bounds. The critical infrastructures can be defined as a complex set of interconnected, interdependent, geographically dispersed systems on which the nation depend as energy distribution, telecommunications, rail, water supply networks etc.

In the literature, there have been several approaches for vulnerability assessment and these approaches can be categorized into two main groups as follows: qualitative approaches and quantitative approaches. Qualitative approaches are generally applied in the sub process of the risk assessment studies (Bajpai and Gupta, 2007). Despite the increasing significance of vulnerability assessment in SRA, researches and analyses using quantitative methodologies have been rarely seen in the literature. Bajpai and Gupta (2005) have shown that security risk status of oil and gas facilities can be assessed qualitatively by developing a security risk factor table and vulnerability assessment worksheet. They divided the facility into various zones and identified the factors that influence the overall security of the facility by rating them on a scale from 0 to 5. Qualitative methods as in Bajpai and Gupta (2005) permit vulnerability ranking or separation into descriptive categories of vulnerability (Garrick et al., 2004). Therefore, qualitative methods can be used to pre-assess the vulnerability but much more is required to quantify the vulnerability.

Generally, existing quantitative methodology studies focused on one kind of critical infrastructure such as energy (Salmeron et al., 2004), telecommunications (Murray et al., 2007), water system (Ezell, 2007). Salmeron et al. (2004) developed a max-min

model to determine the weaknesses in the electric grid to prepare for terrorist attacks. Through decomposition, they solved the problem with a heuristic on two test systems. Murray et al. (2007) presented an optimization approach for identifying interdiction bounds with respect to connectivity and/or flow associated with a system of origins and destinations. They applied this approach to the telecommunications flow in United States. Apostolakis and Lemon (2005) used Multi Attribute Utility Theory (MAUT) for the identification and prioritization of vulnerabilities in an infrastructure that they modelled using interconnected digraphs and employed graph theory to identify the candidate vulnerable scenarios. Ezell (2007) proposed an infrastructure vulnerability assessment model based on MAUT and applied it to a medium-sized clean water system. In this model, the system is presented in a hierarchical structure and clean water system model decomposition serves as the structure of the value model with deterrence, detection, delay, and response value functions used to measure protection for components of the system.

There are also various studies that models critical infrastructure interdependencies. Brown et al. (2004) applied simulation to study the impacts of disruptions and used risk analysis to assess infrastructure interdependencies. Their purpose was to identify infrastructure risks and ways to reduce them. Min et al. (2007) proposed a modelling and analysis framework that uses system dynamics, functional models and nonlinear optimization algorithms to study the entire interconnected system of infrastructures. Their purpose was to simulate the effects of localized capacity losses on the entire integrated system and to predict the extent of the shortage and its impact across the entire system.

From the previous researches, it is observed that vulnerability assessment in SRA is recognized as a worldwide problem. Despite the availability of the researches on this issue, the nature of the problem additionally seeks for the utilization of fuzzy logic in order to deal with the uncertainty and the vagueness of the decision environment in practice. Furthermore, in addition to the physical dependencies of the system functions, the interdependencies among the system functions, logical dependencies, in other words logical vulnerabilities, have to be considered and included into the vulnerability computations. Quantifying the vulnerability of such a system defended against the adversary attack by considering the interdependencies among the functions of the system has not been adequately addressed in the literature. That’s

why; these existing approaches and decision-making models are not satisfying the solution of this problem in a consistent manner. Hence, this chapter addresses a quantified fuzzy approach based on SMART and FCM methodology for managing a more realistic and structured vulnerability assessment process to provide practical solutions in real life applications.

3.3 Theoretical Background for Vulnerability Assessment Modelling

In this section, theoretical background information on triangular fuzzy numbers (TFNs), linguistic variables, fuzzy SMART and FCM methodologies are presented, respectively**.**

3.3.1 Triangular fuzzy number

A fuzzy number is a convex, normalized fuzzy set defined on the real line whose membership function is at least semi continuous and has the functional value $\mu_{\tilde{M}}(x) = 1$ at precisely one element (Ross, 1995). In other words, a fuzzy number is a quantity whose value is imprecise rather than exact. Among the various types of a fuzzy number such as trapezoidal, bell-shaped etc., TFN is the most popular one as it is easy to use and interpret. A TFN is completely represented by a triplet such as $\tilde{M} = (a \mid b,\ b \mid c)$ or $\tilde{M} = (a,\ b,\ c)$ whose membership function can be defined as (Kaufmann and Gupta, 1991)

$$\mu_{\tilde{M}}(x) = \begin{cases} 0, & x<a, \\ \dfrac{(x-a)}{(b-a)}, & a \le x \le b, \\ \dfrac{(c-x)}{(c-b)}, & b \le x \le c, \\ 0, & x>c. \end{cases} \qquad \textbf{(3.1)}$$

The parameters *a*, *b* and *c*, respectively, denote the smallest possible value, the most promising value, and the largest possible value that describe a fuzzy event. A sample TFN, $\tilde{M} = (a,\ b,\ c)$, is shown in Figure 3.1.

The fuzzy algebraic operations (addition, multiplication, division and subtraction) of two TFNs $\tilde{M}_1 = (a_1, b_1, c_1)$ and $\tilde{M}_2 = (a_2, b_2, c_2)$ are applied as expressed within the

contents of various researches (Kaufmann and Gupta, 1991; Chen and Hwang, 1992).

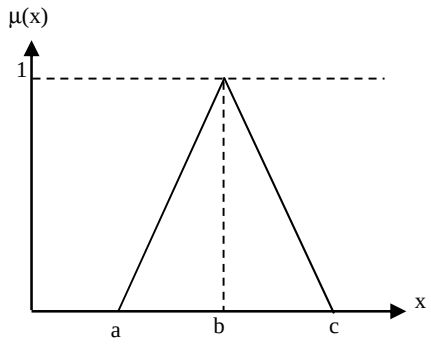


Figure 3.1: A triangular fuzzy number.

The result of fuzzy operations is a fuzzy number and in some situations a single scalar quantity is needed as an output. Therefore, it is required to convert a fuzzy number into a crisp value. There are several available defuzzification methods for this purpose in the literature. Mean of maximum method, centroid method (or centre of area) and α-cut methods are the most common defuzzification methods (Sugeno, 1985; Lee, 1990). Each of these methods has advantages and disadvantages. In this study, the centroid method is utilized due to its simplicity and widespread use. A TFN, $\tilde{M} = (a,b,c)$, is defuzzified by using the following centroid method equation:

$$D(\tilde{M}) = \frac{\int_a^c x\mu_{\tilde{M}}(x)dx}{\int_a^c \mu_{\tilde{M}}(x)dx} = \frac{\int_a^c \left(x\frac{x-a}{b-a}\right)dx + \int_b^c \left(x\frac{c-x}{c-b}\right)dx}{\int_a^c \left(\frac{x-a}{b-a}\right)dx + \int_b^c \left(\frac{c-x}{c-b}\right)dx} = \frac{1}{3}(a+b+c) \qquad \textbf{(3.2)}$$

3.3.2 Linguistic variables

A linguistic variable is a variable whose values are words or sentences in a natural or artificial language (Zadeh, 1975a;b;c). According to Zadeh (1975a;b;c), it is very difficult for conventional quantification to express reasonably those situations that are overtly complex or hard to define; thus, the notion of a linguistic variable is necessary in such situations. Since linguistic variables are not directly mathematically operable, each linguistic variable is associated with a fuzzy number characterizing the meaning of each generic verbal term. In fuzzy set theory, conversion scales are applied to transform linguistic terms into fuzzy numbers.

Determining the number of conversion scales is generally intuitive (Chen and Hwang, 1992).

Since the use of fuzzy logic becomes very important for the decision making problem in this study, linguistic variables are used to express the qualitative judgments such as the relative importance weights of vulnerability criteria, component and function dependency values, the ratings of system components, and the degree of influence (or causal relationships) among system functions. The possible values for these variables are presented in Table 3.1-3.3. For example, the decision makers are asked to describe the degree of influence among system functions using a linguistic variable given in Table 3.3 and each linguistic variable is indicated by a TFN within the interval of [0, 1]. The linguistic variables in Table 3.3 and their membership functions are shown in Figure 3.2.

Table 3.1: Linguistic variables for the importance weights and dependency values.

Linguistic variable	Triangular fuzzy number
Very low (VL)	(0, 0, 0.1)
Low (L)	(0, 0.1, 0.3)
Medium low (ML)	(0.1, 0.3, 0.5)
Medium (M)	(0.3, 0.5, 0.7)
Medium High (MH)	(0.5, 0.7, 0.9)
High (H)	(0.7, 0.9, 1)
Very High (VH)	(0.9, 1, 1)

Table 3.2: Linguistic variables for the ratings of system components.

Linguistic variable	Triangular fuzzy number
Very poor (VP)	(0, 0, 1)
Poor (P)	(0, 1, 3)
Medium Poor (MP)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Medium Good (MG)	(5, 7, 9)
Good (G)	(7, 9, 10)
Very Good (VG)	(9, 10, 10)

Table 3.3: Linguistic variables for causal relationships among system functions.

Linguistic variable	Membership function	Triangular fuzzy number
Very very low (VVL)	μ_{vvl}	(0, 0.1, 0.2)
Very low (VL)	μ_{vl}	(0.1, 0.2, 0.35)
Low (L)	μ_{l}	(0.2, 0.35, 0.5)
Medium (M)	μ_{m}	(0.35, 0.5, 0.65)
High (H)	μ_{h}	(0.5, 0.65, 0.8)
Very high (VH)	μ_{vh}	(0.65, 0.8, 0.9)
Very very high (VVH)	μ_{vvh}	(0.8, 0.9, 1)

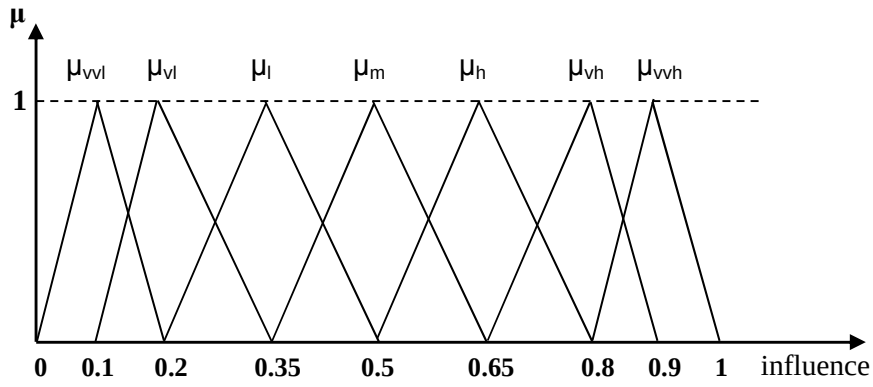


Figure 3.2: Membership functions of linguistic variables for causal relationships.

Besides the decision makers' qualitative judgments, the TFN can also be used to represent the quantitative terms. For example, ''approximately equal to *30*'' can be represented by (*29, 30, 31*); ''approximately between 20 and 24'' can be represented by (*20, 22, 24*); the crisp number *10* can be represented by (*10, 10, 10*) as a special TFN for the fuzzy algebraic operations (Liang, 1999).

3.3.3 The fundamentals of SMART

SMART is a compensatory method of multiple criteria/attribute decision making (MCDM), developed by Edwards in 1971. This method was designed to provide a simple way to implement the beginnings of MAUT. SMART uses the Simple Additive Weight (SAW) method as a basis for obtaining the total values of individual alternatives to rank them according to the order of preference (Edwards, 1971; Edwards, 1977; Edwards and Barron, 1994).

In this method, a score is obtained by adding the contribution from each criterion. Since two items with different measurement units cannot be added, normalization is required to permit addition among criteria values. The total score for each alternative can be computed by multiplying the normalized value of each criterion for the alternatives with the importance weight of the criterion and then summing these products over all the criteria (Yoon and Hwang, 1995). Formally, the total score of an alternative can be expressed as

$$S_i = \sum_{j=1}^{n} w_j r_{ij}, \quad i = 1,2,...m \qquad \textbf{(3.3)}$$

where S_i is the total score of alternative *i*, w_j is the importance weight of criterion *j*, r_{ij} is the normalized rating of the alternative *i* for the criterion *j*, *m* is the number of

alternatives and *n* is the number of criteria. Finally, the alternative with the highest score is selected as the preferred one.

In SMART, weights of criteria and ratings of alternatives are assigned directly using different scales. The simplicity of the questions done to the decision maker and the easiness of the analysis done on the answers are the great advantages of SMART. These issues directly influence on the understanding of the decision maker about the process used in the solution of the problem.

Another advantage of the SMART is that the decision model is independent of the alternatives (Brownlow and Watson, 1987). Since the ratings of alternatives are not relative, changing the number of alternatives considered will not in itself change the decision scores of the original alternatives (Edwards and Barron, 1994). This issue is particularly useful when new alternatives or criteria are needed to be added to the existing decision model. In that case, the evaluation process does not require any further evaluations and can continue from the previous scores obtained.

Furthermore, as the time is a crucial factor for managerial decision making, SMART becomes a better method than the other MCDM methods as it often requires a short period of decision cycle.

Along the years, the SMART has been successfully applied to various MCDM problems and became very popular as its analysis incorporates a wide variety of quantitative and qualitative criteria. Due to many advantages mentioned above, SMART becomes a better choice to evaluate the initial vulnerability of system components, system functions and the system with respect to determined criteria, and to deal with the ratings of both qualitative and quantitative criteria. Hence, in this study, a fuzzy SMART approach proposed by Chou and Chang (2007) in the GDM situation to solve a strategic MCDM problem is utilized.

3.3.4 Brief overview on FCM methodology

FCM methodology is a natural extension to cognitive maps, which can be found in the fields of economics, sociology and political science (Axelrod, 1976; Kosko, 1986). It is originated from the combination of Fuzzy Logic and Neural Networks for modelling complex systems. A FCM describes the behaviour of a system in terms of concepts; each concept represents an entity, a state, a variable or a characteristic of the system (Dickerson and Kosko, 1997). FCMs are used to represent and to model

the knowledge on the examining system. Existing knowledge on the behaviour of the system is stored in the structure of nodes and interconnections of the map. The graphical illustration of an FCM is a signed fuzzy graph with feedback, consisting of nodes and weighted interconnections. Signed and weighted arcs connect various nodes representing the causal relationships that exist among concepts. A simple graphical representation of FCMs is depicted on Figure 3.3.

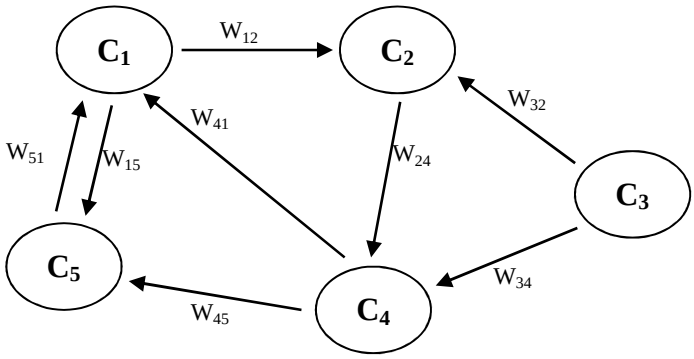


Figure 3.3: A simple fuzzy cognitive map.

In Figure 3.3, C_i is a concept with a state value. The state value can be a fuzzy value within [0, 1] that represents the existent degree of a concept. The weight W_{ij} of an arrow indicates the influence degree from the cause concept C_i to the effect concept C_j, which can be a fuzzy value within [-1, 1]. Positive or negative sign and fuzzy weights (e.g. W_{12}) model the expert knowledge of the causal relationships (Kosko, 1991). Concept C_i causally increases C_j if the weight value $W_{ij} > 0$ and causally decreases C_j if $W_{ij} < 0$. When $W_{ij} = 0$; concept C_i has no causal effect on C_j. In practice, the sign of W_{ij} indicates whether the relationship between concepts is positive or negative, while the value of W_{ij} indicates how strongly concept C_i influences concept C_j. The forward or backward direction of causality indicates whether concept C_i causes concept C_j or vice versa, respectively.

The value of each concept in iterations can be computed from the values of the concepts in the preceding state using the following equation (Xirogiannis et al., 2004):

$$C_i^{t+1} = f\left(C_i^t + \sum_{j=1, j\neq i}^{n} W_{ji} C_j^t\right) \qquad \textbf{(3.4)}$$

where C_i^{t+1} is the value of concept C_i at the step $t + 1$, C_i^t is the value of the interconnected concept C_j at step t, W_{ji} is a corresponding fuzzy weight between two given nodes, from C_j to C_i and f is a given threshold function that transforms the result into a value in the interval where concepts can take values. The threshold function f can be bivalent ($f(x)$= 0 or 1), trivalent ($f(x)$= -1, 0 or 1), tangent hyperbolic ($f(x)=tanh(x)$) or the unipolar sigmoid function ($f(x)=1/(1+e^{-\lambda x})$, where λ is a constant). Hyperbolic function is used when concepts can be negative and their values belong to the interval [-1, 1]. The unipolar sigmoid function where $\lambda > 0$ determines the steepness of the continuous function and is used when the values of the concepts lie within [0, 1]. Thus, we used unipolar sigmoid function in this study and assume that $\lambda = 1$.

The initial values of the concepts in the input vector and the weighted arcs are set to specific values based on the expert's beliefs. Afterwards, the system is free to interact. This interaction continues until the model:

- Reaches equilibrium at a fixed point, with the output values, being decimals in the interval, stabilizing at fixed numerical values.
- Exhibits limit cycle behaviour, with the output values falling in a loop of numerical values under a specific time period.
- Exhibits a chaotic behaviour, with each output value reaching a variety of numerical values in a non-deterministic, random way.

Modelling a system using FCM has several advantages. FCMs are very simple, flexible and powerful tools for analyzing and modelling the real world as a collection of concepts and causal relationships. This simplicity helps the decision makers better understand the underlying formal model and its execution. In addition, they show an abstract representation and are capable of fuzzy reasoning (Stach et al., 2005). Furthermore, even if the initial map of the problem is incomplete or incorrect, further additions to the map can be included, and the effects of new parameters can be quickly seen (Sharif and Irani, 2006a;b). Therefore, FCM is chosen as a modelling approach in this study to simulate the system vulnerability behaviour by taking into account the possible interrelationships among the system functions.

3.4 Fuzzy Integrated Vulnerability Assessment Model

The proposed FIVAM framework in this study is based on fuzzy set theory, SMART and FCM methodology in the GDM environment. In this integrated utilization, fuzzy SMART is used as a simple and effective MCDM technique to weight the vulnerability criteria and to calculate the initial vulnerability value of the components with respect to these weighted criteria. After calculating the initial vulnerability values of all components, the physical dependencies of functions on components and the logical dependencies of system on functions are determined. Then, the initial vulnerability values of both the functions and the system are computed using these dependencies and component vulnerability values ignoring the possible interdependencies among the system functions. In the next phase, FCM methodology is applied to simulate the system vulnerability behaviour depending on the vulnerabilities and the interdependencies among the system functions. After calculating the vulnerability values of the functions in the long run by using FCM, the system function and component vulnerabilities are recalculated by considering the effects of these possible interdependencies among the system functions. According to these results, the most critical functions and components in the system are determined and ranked. Finally, the vulnerabilities before and after the FCM simulation are compared and evaluated. The proposed approach consists of the following steps is shown in Figure 3.4.

Step 1: Form a working group. The group size influences the effectiveness of the GDM. As Yetton and Bottger (1983) pointed out groups of five are the most effective and odd numbered groups help avoid decision deadlocks.

Assume that there is a group of *s* decision makers/experts (DMs) (D_i , i =*1, 2, ..., s*) who are responsible for all the activities in the vulnerability assessment process.

Step 2: Characterize the system defended. The DMs organize series of meetings for identifying the system functions and system components considering the system mission and system boundaries. Then, a hierarchical system structure is constructed using this information.

Assume that there are t system functions (F_j, j =1, 2, ..., t) and there are u_{F_j} system components (T_{jk}, j =1, 2, ..., t , k = 1, 2, …, u_{F_j}) that are required by function F_j to work properly.

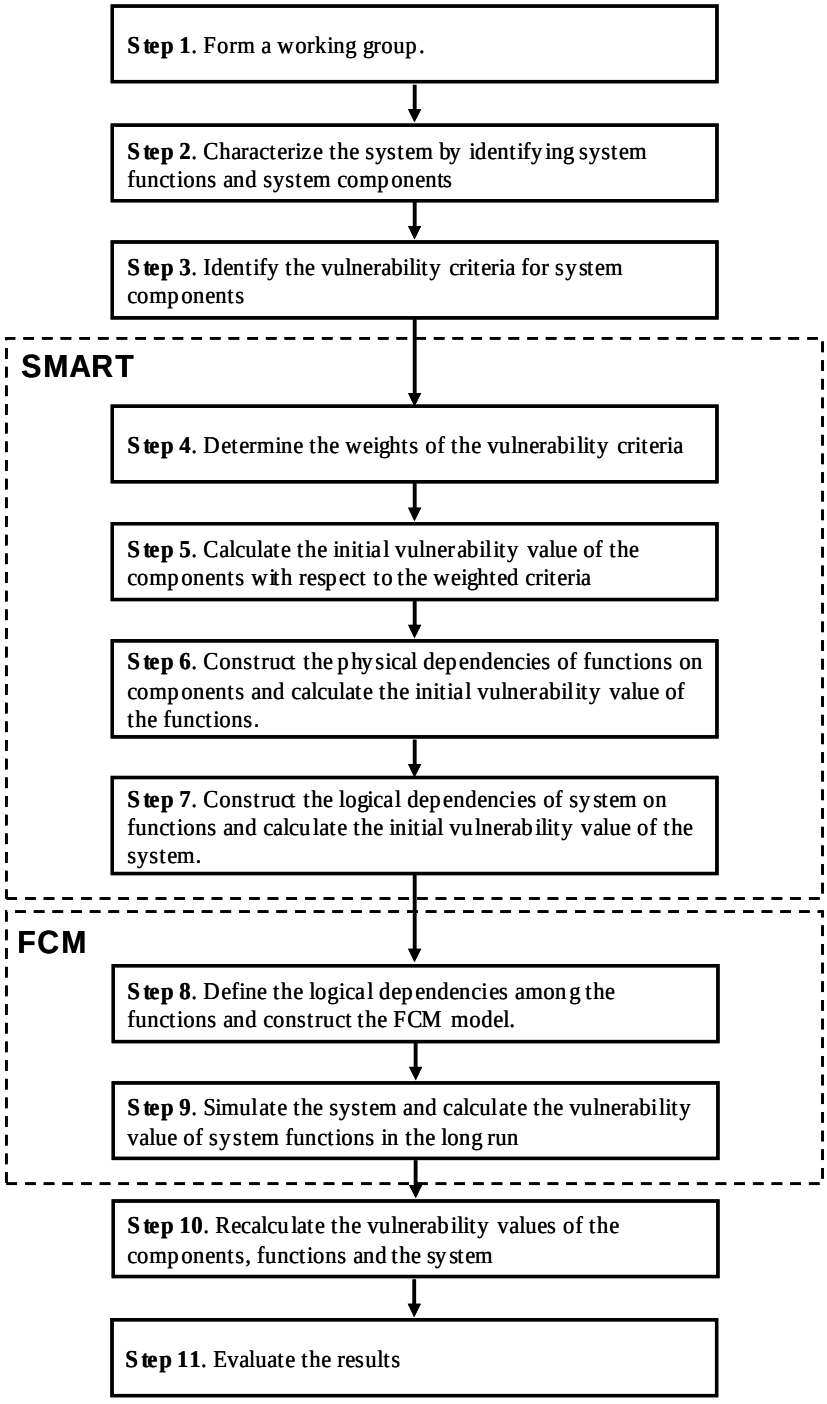


Figure 3.4: The steps of FIVAM approach.

Step 3: Identify the vulnerability criteria for system components. The DMs use brainstorming GDM method for identifying the relevant criteria of the internal and external environment on vulnerability assessment of components. Then, these criteria

are categorized as qualitative or quantitative, and quantitative criteria are also categorized as cost or benefit (polarity).

Let C_l, $l = 1, 2, \ldots, v$ be the vulnerability criteria.

Step 4: Determine the weights of the vulnerability criteria. Each DM assigns linguistic weighting variables shown in Table 3.1 for each criterion. Then, these fuzzy values are aggregated and the relative importance of the criteria is determined.

Let $\tilde{W}_{il} = (a_{il}, b_{il}, c_{il})$, $i = 1,2,...,s$, $l = 1,2,...v$ be the TFN corresponding to the linguistic variable given to criterion C_l by decision maker D_i. The aggregated fuzzy criterion weight, $\tilde{W}_{C_l} = (a_{C_l}, b_{C_l}, c_{C_l})$, $l = 1,2,...v$, of criterion C_l assessed by the group of s DMs is calculated as follows:

$$\tilde{W}_{C_l} = \frac{1}{s} \otimes \sum_{i=1}^{s} \tilde{W}_{il} \qquad \textbf{(3.5)}$$

where $a_{C_l} = \frac{1}{s} \otimes \sum_{i=1}^{s} a_{il}$, $b_{C_l} = \frac{1}{s} \otimes \sum_{i=1}^{s} b_{il}$ and $c_{C_l} = \frac{1}{s} \otimes \sum_{i=1}^{s} c_{il}$. Then, the defuzzification of $\tilde{W}_{C_l}$, denoted by $d(\tilde{W}_{C_l})$ is calculated using Eq.3.2 as follows:

$$d(\tilde{W}_{C_l}) = \frac{1}{3}(a_{C_l} + b_{C_l} + c_{C_l}),\ l = 1,2,...,v \qquad \textbf{(3.6)}$$

As the fuzzy SMART requires cardinal weights that are normalized to sum to 1, the crisp value of weight for criterion C_l, denoted as W_{C_l}, is given by

$$W_{C_l} = \frac{d(\tilde{W}_{C_l})}{\sum_{l=1}^{v} d(\tilde{W}_{C_l})},\ l = 1,2,...,v \qquad \textbf{(3.7)}$$

where $\sum_{l=1}^{v} W_{C_l} = 1.$

Step 5: Calculate the initial vulnerability value of the components with respect to the weighted criteria. The DMs use linguistic rating variables shown in Table 3.2 to assess fuzzy ratings of components with respect to vulnerability criteria, and then compute aggregated fuzzy ratings. While calculating the initial vulnerability value of

the components, it is assumed that the vulnerability of any component does not affect the vulnerability of the other components.

Let $\tilde{x}_{ijkl} = (a_{ijkl}, b_{ijkl}, c_{ijkl}),\ i = 1,2,...,s,\ j = 1,2,...,t,\ k = 1,2,...,u_{F_j},\ l = 1,2,...v$ be the linguistic rating assigned to the component T_{jk} of function F_j for qualitative/subjective criterion C_l by decision maker D_i. Similarly, let $\tilde{q}_{ijkl} = (d_{ijkl}, e_{ijkl}, f_{ijkl}),\ i = 1,2,...,s,\ j = 1,2,...,t,\ k = 1,2,...,u_{F_j},\ l = 1,2,...v$ be the TFN (or crisp) cost or benefit value assessed to the component T_{jk} of function F_j for quantitative/objective criterion C_l by decision maker D_i. The following equations are applied to normalize the quantitative value.

$$\tilde{x}_{ijkl} = \frac{\tilde{q}_{ijkl} - \min_{jk}\{d_{ijkl}\}}{\max_{jk}\{f_{ijkl}\} - \min_{jk}\{d_{ijkl}\}} \otimes 10 \qquad \textbf{(3.8)}$$

where $\tilde{x}_{ijkl}$ denotes the normalized fuzzy rating of fuzzy benefit $\tilde{q}_{ijkl}$.

$$\tilde{x}_{ijkl} = \frac{\max_{jk}\{f_{ijkl}\} - \tilde{q}_{ijkl}}{\max_{jk}\{f_{ijkl}\} - \min_{jk}\{d_{ijkl}\}} \otimes 10 \qquad \textbf{(3.9)}$$

where $\tilde{x}_{ijkl}$ denotes the normalized fuzzy rating of fuzzy cost $\tilde{q}_{ijkl}$. The aggregated fuzzy rating, $\tilde{x}_{jkl} = (a_{jkl}, b_{jkl}, c_{jkl}),\ j = 1,2,...,t, k = 1,2,...,u_{F_j},\ l = 1,2,...v$, of component T_{jk} for criterion C_l is calculated as

$$\tilde{x}_{jkl} = \frac{1}{s} \otimes \sum_{i=1}^{s} \tilde{x}_{ijkl} \qquad \textbf{(3.10)}$$

Then, the initial fuzzy vulnerability value of component k of function j, $\tilde{V}_{T_{jk}}$, can be obtained by:

$$\tilde{V}_{T_{jk}} = \sum_{l=1}^{v} W_{C_l} \otimes \tilde{x}_{jkl},\ j = 1,2,...,t,\ k = 1,2,...,u_{F_j} \qquad \textbf{(3.11)}$$

where $\tilde{V}_{T_{jk}} = (a_{jk}, b_{jk}, c_{jk}),\ j = 1,2,...,t,\ k = 1,2,...,u_{F_j}$.

The component vulnerability value $\tilde{V}_{T_{jk}}$ is defuzzified using Eq.3.2 and component vulnerability value $d(\tilde{V}_{T_{jk}})$ is determined. Then, normalized crisp component vulnerability value $V_{T_{jk}}$ is calculated as follows:

$$V_{T_{jk}} = \frac{d(\tilde{V}_{T_{jk}})}{\max_{jk}\left(d(\tilde{V}_{T_{jk}})\right)},\ j = 1,2,...,t\ ,\ k = 1,2,...,u_{F_j} \qquad \textbf{(3.12)}$$

Step 6: Construct the physical dependencies of functions on components and calculate the initial vulnerability value of the functions. To determine the initial function vulnerabilities that depend on component vulnerability values, the DMs assign linguistic variables shown in Table 3.1 for the degree of dependency between function and component.

Let $\tilde{W}_{ijk} = (a_{ijk}, b_{ijk}, c_{ijk}),\ i = 1,2,...,s\ ,\ j = 1,2,...,t\ ,\ k = 1,2,...,u_{F_j}$ be the TFN corresponding to the linguistic variable given to the dependency degree of function F_j on component T_{jk} by decision maker D_i. The aggregated fuzzy dependency degree, $\tilde{W}_{T_{jk}} = (a_{T_{jk}}, b_{T_{jk}}, c_{T_{jk}}),\ j = 1,2,...,t\ ,\ k = 1,2,...,u_{F_j}$ of component T_{jk} assessed by the group of s DMs is determined as:

$$\tilde{W}_{T_{jk}} = \frac{1}{s} \otimes \sum_{i=1}^{s} \tilde{W}_{ijk} \qquad \textbf{(3.13)}$$

Then, the defuzzified dependency degree, $d(\tilde{W}_{T_{jk}})$, is calculated using Eq.3.2 and normalized as follows:

$$W_{T_{jk}} = \frac{d(\tilde{W}_{T_{jk}})}{\sum_{k=1}^{u_{F_j}} d(\tilde{W}_{T_{jk}})},\ j = 1,2,...,t \qquad \textbf{(3.14)}$$

where $\sum_{k=1}^{u_{F_j}} W_{T_{jk}} = 1\ ,\ j = 1,2,...,t$.

The initial fuzzy vulnerability value for function F_j, denoted as $\tilde{V}_{F_j}$, is the sum product of all component vulnerability values and their associated dependency degree as follows:

$$\tilde{V}_{F_j} = \sum_{k=1}^{u_{F_j}} \left(W_{T_{jk}} \otimes \tilde{V}_{T_{jk}} \right),\ j = 1,2,...,t \qquad \textbf{(3.15)}$$

where $\tilde{V}_{F_j} = (a_j, b_j, c_j),\ j = 1,2,...,t.$

Since, the threshold function in FCM model requires crisp concept values within [0, 1], normalized crisp function vulnerability value V_{F_j} is calculated as follows:

$$V_{F_j} = \frac{d(\tilde{V}_{F_j})}{\max_j \left(d(\tilde{V}_{F_j}) \right)},\ j = 1,2,...,t \qquad \textbf{(3.16)}$$

where $d(\tilde{V}_{F_j})$ is the defuzzified function vulnerability value.

Step 7: Construct the logical dependencies of system on functions and calculate the initial vulnerability value of the system. To determine the system vulnerability that depends on function vulnerability values, the DMs assign linguistic variables shown in Table 3.1 for the degree of dependency between system and function.

Let $\tilde{W}_{ij} = (a_{ij}, b_{ij}, c_{ij}),\ i = 1,2,...,s\ ,\ j = 1,2,...,t$ be the TFN corresponding to the linguistic variable given to the dependency degree of system on function F_j by decision maker D_i. The aggregated fuzzy dependency degree, $\tilde{W}_{F_j} = (a_{F_j}, b_{F_j}, c_{F_j}),\ j = 1,2,...,t$ of component F_j assessed by the group of s DMs is defined as:

$$\tilde{W}_{F_j} = \frac{1}{s} \otimes \sum_{i=1}^{s} \tilde{W}_{ij} \qquad \textbf{(3.17)}$$

As in the previous steps, the fuzzy dependency degree, $\tilde{W}_{F_j}$, is defuzzified and normalized value, $\tilde{W}_{F_j}$, is calculated. Then, the vulnerability value for the system S, denoted as V_S, is the sum product of all function vulnerability values and their associated dependency degree as follows:

$$V_S = \sum_{j=1}^{t} \left(W_{F_j} \otimes V_{F_j} \right) \qquad \textbf{(3.18)}$$

Step 8: Define the logical dependencies among the functions and construct the FCM model. The DMs use linguistic influence variables shown in Table 3.3 to assess fuzzy causal relationships (influences) among the system functions.

Let $\tilde{r}_{ijm} = (a_{ijm}, b_{ijm}, c_{ijm})$, $i = 1,2,...,s$, $j, m = 1,2,...,t$ be the TFN corresponding to the linguistic variable assigned to the influence degree of function F_j to function F_m by decision maker D_i. The aggregated fuzzy influence value, $\tilde{r}_{jm} = (a_{jm}, b_{jm}, c_{jm})$, $j, m = 1,2,...,t$ where $\tilde{r}_{jj} = 0$, is calculated as:

$$\tilde{r}_{jm} = \frac{1}{s} \otimes \sum_{i=1}^{s} \tilde{r}_{ijm} \qquad \textbf{(3.19)}$$

As the unipolar sigmoid function in FCM model requires crisp values, the crisp influence value r_{jm} is determined by defuzzifying the aggregated fuzzy influence value $\tilde{r}_{jm}$ using Eq.3.2.

Step 9: Simulate the system and calculate the vulnerability value of the system functions in the long run. The vulnerability value of a system function in each iteration is calculated using Eq.3.4 as follows:

$$V_{F_j}{}^{z+1} = f\left(V_{F_j}{}^{z} + \sum_{m=1, m\neq j}^{t} r_{mj} V_{F_m}{}^{z} \right), \; j = 1,2,...,t \qquad \textbf{(3.20)}$$

When the model reaches equilibrium at a fixed point after some iterations, new crisp vulnerability value of for function F_j, denoted as $V_{F_j}^{e}$, is determined.

Step 10: Recalculate the vulnerability values of the components, functions and the system. As the result of the FCM simulation is the function vulnerabilities at the equilibrium point, first of all, the hidden vulnerability of the functions have to be determined. If function F_j influences function F_m, there is a hidden vulnerability on cause function F_j because of the dependency of F_m on F_j. This hidden vulnerability $V_{F_j}^{h}$ of a function F_j is calculated as

$$V_{F_j}^{h} = \sum_{m=1, m\neq j}^{t} \left(r_{jm} V_{F_m}^{e} \right), \; j = 1,2,...,t. \qquad \textbf{(3.21)}$$

Then, the real vulnerability value of function F_j is the sum of initial and the hidden vulnerabilities as follows:

$$V'_{F_j} = V_{F_j} + V^h_{F_j},\ j = 1,2,...,t. \quad \textbf{(3.22)}$$

The hidden vulnerability value of the system, V^h_S, is calculated by the sum product of hidden function vulnerability values and their associated dependency degree as

$$V^h_S = \sum_{j=1}^{t} \left(W_{F_j} * V^h_{F_j} \right) \quad \textbf{(3.23)}$$

The real vulnerability value of the system, V'_S, is therefore given by

$$V'_S = V_S + V^h_S \quad \textbf{(3.24)}$$

Similarly, the hidden function vulnerabilities calculated by the FCM simulation have to be reflected to the component vulnerabilities proportional to the component-function dependencies. To do this, the vulnerability values of the components are recalculated by the following equations:

$$V^h_{T_{jk}} = W_{T_{jk}} * V^h_{F_j},\ j = 1,2,...,t,\ k = 1,2,...,u_{F_j} \quad \textbf{(3.25)}$$

$$V'_{T_{jk}} = V_{T_{jk}} + V^h_{T_{jk}},\ j = 1,2,...,t,\ k = 1,2,...,u_{F_j} \quad \textbf{(3.26)}$$

Step 11: Evaluate the results. The system components and functions based on their vulnerability values before and after FCM simulation are ranked and compared. Furthermore, the hidden vulnerabilities are presented and discussed.

The detailed descriptions of each step are elaborated in the following illustrative case study section.

3.5 An Illustrative Example for Vulnerability Assessment

In this section, the proposed FIVAM approach as described in Section 4 is applied to a hypothetical Airport X to discover hidden vulnerabilities for improving its site security. When the security requirements are considered against the possible terrorist attacks, the challenge of vulnerability assessment for an airport becomes very complicated.

Note that all the values used throughout this example are purely generic and notional. Even though this case study is very simple and the results may not increase our

knowledge about the system, it validates the FIVAM approach. A step-by-step algorithm for this example is as follows:

Step 1: In this case study, the number of DMs who were involved in the decision-making process is selected as five. In order to extend the assessment to account for the conflicts among different interest groups who have different objectives, goals and criteria; one terrorism expert, one security expert, two representatives from the airport administration and one academician from the Faculty of Aeronautics have participated in the decision process as DMs.

In the evaluation process, while the terrorism and security experts mostly deal with the security issues, representatives from an airport administration and the academician concern the functionality of Airport X. The authors support these DMs with their technical knowledge on the methodology. Series of meetings were organized with participation of these DMs and all the issues including comments and suggestions are discussed at these meetings.

Step 2: The DMs identified the relevant functions and components of Airport X by considering the following three questions: "What is the principal mission of Airport X?", "What system functions are essential to carry out this mission by Airport X?" and "What system components do these system functions depend on for their success?". For simplification, only the critical functions have been considered and their most relevant components have been focused on at the component abstraction level in this study.

In order to accomplish its mission, the DMs determined that Airport X has to provide six main functions: (1) Ground handling service (GHS) for servicing, maintenance and engineering of aircrafts; (2) Passenger service (PS) for gate-management, check-in desk allocation, and flight-information displays; (3) Cargo and baggage service (CBS) function for transportation of payload; (4) Air traffic management service (ATMS) for approach, landing, taxiing, take off and departure of aircrafts; (5) Emergency services (ES) for fire fighting, medical and security services; and (6) Infrastructure services (IS) for maintaining the general service capability of the airport.

After identifying the relevant functions of Airport X, the DMs determined 20 system components by answering the third question mentioned above. Table 3.4 summarizes

the functions and the components of Airport X in a hierarchical structure and Figure 1.6 illustrates the sketch of Airport X.

Table 3.4: Hierarchical system structure of airport X.

Components		Functions		System
T_{11}	Airfield Maintenance Building	F_1	Ground Handling Service (GHS)	Airport X (S)
T_{12}	Fuel Complex Building			
T_{21}	Passenger Terminal	F_2	Passenger Service (PS)	
T_{22}	Parking Facility			
T_{23}	Bus Station			
T_{31}	Custom Building	F_3	Cargo and Baggage Service (CBS)	
T_{32}	Cargo Terminal			
T_{41}	Air Traffic Control and Tower	F_4	Air Traffic Management Service (ATMS)	
T_{42}	Apron			
T_{43}	Runway and Taxiway			
T_{51}	Main Entrance and Security Control Building	F_5	Emergency Service (ES)	
T_{52}	Security Building			
T_{53}	Aircraft Rescue and Fire Fighting Building			
T_{54}	Police Station Building			
T_{55}	Fuel Complex Guard Building			
T_{56}	Guard Tower			
T_{57}	Fencing			
T_{61}	Heating Centre Building	F_6	Infrastructure Service (IS)	
T_{62}	Power Centre Building			
T_{63}	Water Storage Building			

Step 3: In this study, the key factors for assessing the vulnerability of Airport X are derived from literature reviews, comprehensive investigation and consultation with DMs. After a comprehensive discussion, all the evaluation criteria for the component vulnerability assessment are identified accordingly. The five DMs collectively set up five criteria and the detail descriptions of these criteria are listed below:

- Deterrence (C_1): Deterrence is defined as defence methods implemented that are perceived by terrorists as too difficult to defeat. The presence of security controls such as access control, perimeter protection, proper lighting and use of metal detector/X-ray/Closed Circuit Television at entrance and at all critical locations increase the deterrence of the component by lowering the attractiveness of a component as a target.
- Detection (C_2): Detection is defined as the capability of determining that an unauthorized terrorist action has occurred or is occurring, including: sensing,

communicating alarm to control centre, and assessing the alarm (Ezell, 2007). The high value of detection decreases the vulnerability of a component.

- Delay (C_3): Delay is defined as the time that an element of a physical protection system is designed to impede terrorist penetration into or exit from the protected area (Ezell, 2007). Decreasing the delay will reduce the potential for a component to be a target.
- Response (C_4): Response is defined as a time to respond to a threat. Response activities occurred immediately after a terrorist attack includes stabilizing affected areas, immediate medical care and evacuation during the terrorist attack. Short response time decreases the vulnerability of a component.
- Recovery (C_5): Recovery is defined as a time to return the affected areas and persons to their pre-event status. It includes restoring critical elements, assisting affected persons, and coordinating relief efforts after the possible terrorist attacks for the worst case scenario. Quicker recovery of a component from an attack indicates that the component is less vulnerable.

As a result, Deterrence (C_1) and Detection (C_2) are the qualitative criteria; whereas Delay (C_3), Response (C_4) and Recovery (C_5) are the quantitative benefit criteria.

Step 4: The linguistic weighting variables (Table 3.1) and their respective fuzzy numbers for DMs are then used to assess the importance weights of the evaluation criteria. These assigned fuzzy values are aggregated by arithmetic mean method using Eq.3.1 and the fuzzy weights of individual criteria can then be determined (Table 3.5). Furthermore, crisp and normalized weight values are also calculated by using Eqs. 3.2-3.3 and included in the table.

Table 3.5: The relative importance weights of the five criteria by five DMs.

Criteria	Polarity	DM's linguistics weights					Aggregated weights		
		DM_1	DM_2	DM_3	DM_4	DM_5	Fuzzy number	Defuzzified	Normalized
C_1	-	H	H	VH	MH	M	(0.62, 0.8, 0.92)	0.780	0.275
C_2	-	H	MH	M	M	ML	(0.38, 0.58, 0.76)	0.573	0.202
C_3	+	M	ML	L	M	ML	(0.16, 0.34, 0.54)	0.347	0.122
C_4	+	MH	M	H	M	MH	(0.46, 0.66, 0.84)	0.653	0.231
C_5	+	M	VL	H	M	M	(0.32, 0.48, 0.64)	0.480	0.169

Polarity : '+' = benefit criteria, '-' = cost criteria

The weights of the criteria presented in Table 3.5 reveal that the most important criteria for assessing vulnerability of a component is "deterrence" ($W_{C_1} = 0.275$); whereas the least important criteria is "delay" ($W_{C_3} = 0.122$).

Step 5: The linguistic rating variables (Table 3.2) and their respective fuzzy numbers for DMs are used to assess the fuzzy ratings of the 20 components with respect to each qualitative/quantitative criterion. As the DMs sometimes have different understandings of the same performance data, the DMs adopted linguistic terms in Table 2 to express their opinions about the rating of every component regarding each quantitative criterion, Delay (C_3), Response (C_4), and Recovery (C_5) in this case study. For instance, some DMs might think that 3 minutes was a ''good'' or ''very good'' delay for "Air Traffic Control and Tower" component, while the others might think that value was ''fair'' or ''medium poor''. Alternatively, in accordance with crisp data, the normalized values of individual quantitative criteria can be computed by using Eq.3.3 or Eq.3.5. The aggregated fuzzy rating of each criterion can be computed by Eq.3.6, and then, the aggregated fuzzy ratings are formed. The fuzzy vulnerability values of components are obtained using Eq.3.7 and the results are listed in Table 3.6. Furthermore, crisp and normalized vulnerability values of components and their rankings are also calculated by using Eq.3.8 and included in the table.

Table 3.6: Aggregated fuzzy ratings and vulnerability of components.

	Aggregated fuzzy ratings regarding each criterion					**Component vulnerability value**			
	C_1	**C_2**	**C_3**	**C_4**	**C_5**	**Fuzzy number**	**Defuz.**	**Norm.**	**Rank**
T_{11}	(2.6, 4.6, 6.6)	(1.8, 3.2, 5)	(4.6, 6.6, 8.4)	(5, 7, 8.6)	(4.6, 6.6, 8.4)	(3.58, 5.45, 7.26)	5.430	0.904	5
T_{12}	(3, 5, 7)	(3.2, 5, 7)	(3.4, 5.4, 7.4)	(3.8, 5.8, 7.8)	(4.2, 6.2, 8.2)	(3.48, 5.44, 7.44)	5.450	0.907	4
T_{21}	(4.6, 6.6, 8.4)	(0.2, 1.2, 3)	(0.2, 1.2, 3)	(2, 3.8, 5.8)	(6.6, 8.4, 9.6)	(2.91, 4.51, 6.25)	4.556	0.758	9
T_{22}	(1, 2.6, 4.6)	(5.8, 7.6, 8.8)	(3, 5, 7)	(2.2, 4.2, 6.2)	(0.2, 1.2, 3)	(2.36, 4.04, 5.84)	4.079	0.679	11
T_{23}	(0.8, 2.6, 4.6)	(5, 7, 8.6)	(4.6, 6.6, 8.4)	(3.4, 5.4, 7.4)	(0.2, 1.2, 3)	(2.61, 4.39, 6.25)	4.417	0.735	10
T_{31}	(3, 5, 7)	(4.2, 6.2, 8.2)	(4.2, 6.2, 8)	(1.8, 3.8, 5.8)	(1, 2.4, 4.2)	(2.77, 4.67, 6.61)	4.687	0.780	8
T_{32}	(2.6, 4.6, 6.6)	(5, 7, 8.8)	(5, 7, 8.8)	(4.2, 6.2, 8.2)	(0.8, 2, 3.8)	(3.44, 5.31, 7.21)	5.320	0.886	6
T_{41}	(3.8, 5.8, 7.6)	(0.4, 1.8, 3.8)	(0.4, 1.6, 3.4)	(2.6, 4.6, 6.6)	(7.4, 9, 9.8)	(3.03, 4.74, 6.46)	4.744	0.790	7
T_{42}	(1, 2.6, 4.6)	(5.4, 7.4, 9)	(1.2, 3, 5)	(2.6, 4.6, 6.6)	(0, 0.4, 1.8)	(2.11, 3.71, 5.53)	3.783	0.630	12
T_{43}	(1, 2.6, 4.6)	(3.4, 5.4, 7.4)	(2.2, 4.2, 6.2)	(3, 5, 7)	(0.2, 1.2, 3)	(1.96, 3.68, 5.64)	3.760	0.626	13
T_{51}	(0, 0.4, 1.8)	(0, 0.2, 1.4)	(0, 0.2, 1.4)	(0, 0.4, 1.8)	(0.8, 2.2, 4.2)	(0.14, 0.64, 2.08)	0.951	0.158	20
T_{52}	(0, 0.2, 1.4)	(0, 0.2, 1.4)	(0, 0, 1)	(0, 0.2, 1.4)	(1.8, 3.8, 5.8)	(0.3, 0.79, 2.1)	1.062	0.177	19
T_{53}	(1.6, 3.4, 5.4)	(0.6, 2.2, 4.2)	(0.2, 1, 2.6)	(1.2, 3, 5)	(1, 2.6, 4.6)	(1.03, 2.64, 4.59)	2.752	0.458	14
T_{54}	(0, 0.2, 1.4)	(0, 0.4, 1.8)	(0, 0.2, 1.4)	(0.2, 1, 2.6)	(2.6, 4.6, 6.6)	(0.49, 1.17, 2.64)	1.432	0.238	16
T_{55}	(0, 0.6, 2.2)	(0.4, 1.8, 3.8)	(0.4, 1.4, 3)	(0, 0.6, 2.2)	(0.2, 1.2, 3)	(0.16, 1.04, 2.76)	1.321	0.220	17
T_{56}	(0, 0.6, 2.2)	(0.4, 1.8, 3.8)	(0.2, 1.2, 3)	(0, 0.6, 2.2)	(0, 0.4, 1.8)	(0.11, 0.88, 2.55)	1.181	0.197	18
T_{57}	(0, 0.6, 2.2)	(0.2, 1.2, 3)	(3.8, 5.8, 7.8)	(0.2, 1.4, 3.4)	(0, 0.2, 1.4)	(0.55, 1.47, 3.19)	1.738	0.289	15
T_{61}	(3, 5, 7)	(3.8, 5.8, 7.6)	(2.6, 4.6, 6.6)	(2.6, 4.6, 6.6)	(7, 8.8, 9.8)	(3.7, 5.66, 7.45)	5.606	0.933	2
T_{62}	(3.8, 5.8, 7.8)	(3, 5, 7)	(3.8, 5.8, 7.8)	(3, 5, 7)	(7.8, 9.4, 10)	(4.13, 6.06, 7.83)	6.007	1.000	1
T_{63}	(2.6, 4.6, 6.6)	(3.4, 5.4, 7.4)	(3.4, 5.4, 7.4)	(2.6, 4.6, 6.6)	(7.4, 9, 9.8)	(3.67, 5.61, 7.4)	5.560	0.926	3

In Table 3.6, it is identified that the three most vulnerable components are "Power Centre Building" ($V_{T_{62}} = 1.000$), "Heating Centre Building" ($V_{T_{61}} = 0.933$) and "Water Storage Building" ($V_{T_{63}} = 0.926$); whereas the three least vulnerable components are "Main Entrance and Security Control Building" ($V_{T_{51}} = 0.158$), "Security Building" ($V_{T_{52}} = 0.177$) and "Guard Tower" ($V_{T_{56}} = 0.197$). These are the most and the least probable possible targets for the terrorist attacks.

Step 6: In this step, the DMs use the linguistic weighting variables in Table 3.1 to assess the physical degree of dependency between functions and components. These assigned fuzzy values are aggregated and defuzzified using Eqs.3.9-3.10 and the crisp dependency degrees (weights) are determined (Table 3.7). The fuzzy vulnerability values of functions are then calculated by the sum product of all component vulnerability values and their associated dependency degrees using Eq.3.11 (Table 3.7). In addition to this, crisp and normalized vulnerability values of functions and their rankings are also computed using Eq.3.12 and included in the table.

Table 3.7: Dependency degree of components and vulnerability of functions.

Func.	Comp.	Aggregated degree of dependency			Function vulnerability value			
		Fuzzy number	Defuzzified	Normalized	Fuzzy number	Defuzzified	Normalized	Rank
F_1	T_{11}	(0.66, 0.84, 0.96)	0.82	0.52	(3.53, 5.45, 7.35)	5.440	0.932	2
	T_{12}	(0.58, 0.78, 0.92)	0.76	0.48				
F_2	T_{21}	(0.82, 0.96, 1)	0.93	0.73	(2.79, 4.42, 6.19)	4.470	0.766	4
	T_{22}	(0.04, 0.16, 0.34)	0.18	0.14				
	T_{23}	(0.04, 0.14, 0.3)	0.16	0.13				
F_3	T_{31}	(0.38, 0.58, 0.78)	0.58	0.42	(3.16, 5.04, 6.96)	5.051	0.865	3
	T_{32}	(0.62, 0.8, 0.94)	0.79	0.58				
F_4	T_{41}	(0.82, 0.96, 1)	0.93	0.50	(2.52, 4.22, 6.03)	4.256	0.729	5
	T_{42}	(0.16, 0.34, 0.54)	0.35	0.19				
	T_{43}	(0.38, 0.58, 0.78)	0.58	0.31				
F_5	T_{51}	(0.46, 0.66, 0.84)	0.65	0.21	(0.38, 1.17, 2.74)	1.429	0.245	6
	T_{52}	(0.38, 0.58, 0.76)	0.57	0.19				
	T_{53}	(0.26, 0.46, 0.66)	0.46	0.15				
	T_{54}	(0.26, 0.46, 0.66)	0.46	0.15				
	T_{55}	(0.1, 0.26, 0.46)	0.27	0.09				
	T_{56}	(0.26, 0.46, 0.66)	0.46	0.15				
	T_{57}	(0.04, 0.16, 0.34)	0.18	0.06				
F_6	T_{61}	(0.1, 0.24, 0.42)	0.25	0.19	(3.95, 5.89, 7.67)	5.838	1.000	1
	T_{62}	(0.62, 0.82, 0.96)	0.80	0.60				
	T_{63}	(0.1, 0.26, 0.46)	0.27	0.21				

In Table 3.7, it is seen that the most vulnerable function is “Infrastructure Service (IS)” ($V_{F_6} = 1.000$). On the other hand, the least vulnerable function is “Emergency Service (ES)” ($V_{F_5} = 0.245$).

Step 7: The DMs assign the linguistic weighting variables in Table 3.1 for the logical degree of dependency between Airport X and its functions. These assigned fuzzy values are aggregated using Eq.3.13. The crisp vulnerability value of Airport X is then calculated by the sum product of all function vulnerability values and their associated aggregated dependency degrees using Eq.3.14 (Table 3.8). As seen from the table, the Airport X has a vulnerability value of 0.749. By the end of this step, vulnerability assessment is conducted using the SMART approach like the other classical models. However, in the next steps FCM is applied to identify and determine the real and hidden vulnerabilities caused by the functional interdependencies among the system functions.

Table 3.8: Dependency degree of functions and vulnerability value of airport X.

Func.	Aggregated degree of dependency			System vulnerability value
	Fuzzy number	Defuzzified	Normalized	
F_1	(0.42, 0.62, 0.82)	0.62	0.15	0.749
F_2	(0.7, 0.88, 0.98)	0.85	0.21	
F_3	(0.34, 0.54, 0.74)	0.54	0.13	
F_4	(0.74, 0.9, 0.98)	0.87	0.22	
F_5	(0.42, 0.62, 0.8)	0.61	0.15	
F_6	(0.34, 0.54, 0.74)	0.54	0.13	

Step 8: The linguistic influence variables (Table 3.3) and their respective fuzzy numbers for DMs are then used to define the causal relationships among the functions of Airport X. These fuzzy values are aggregated by using Eq.3.15 and crisp influence matrix is constructed after defuzzication for the FCM simulation (Table 3.9). Furthermore, the FCM model for the functions of Airport X is presented in Figure 3.5.

Table 3.9: Causal relationships among the functions of airport X.

Functions	F_1	F_2	F_3	F_4	F_5	F_6
F_1	0.00	0.36	0.00	0.27	0.00	0.00
F_2	0.00	0.00	0.00	0.25	0.00	0.00
F_3	0.00	0.27	0.00	0.00	0.00	0.00
F_4	0.00	0.64	0.00	0.00	0.00	0.00
F_5	0.67	0.44	0.35	0.59	0.00	0.64
F_6	0.56	0.38	0.27	0.38	0.50	0.00

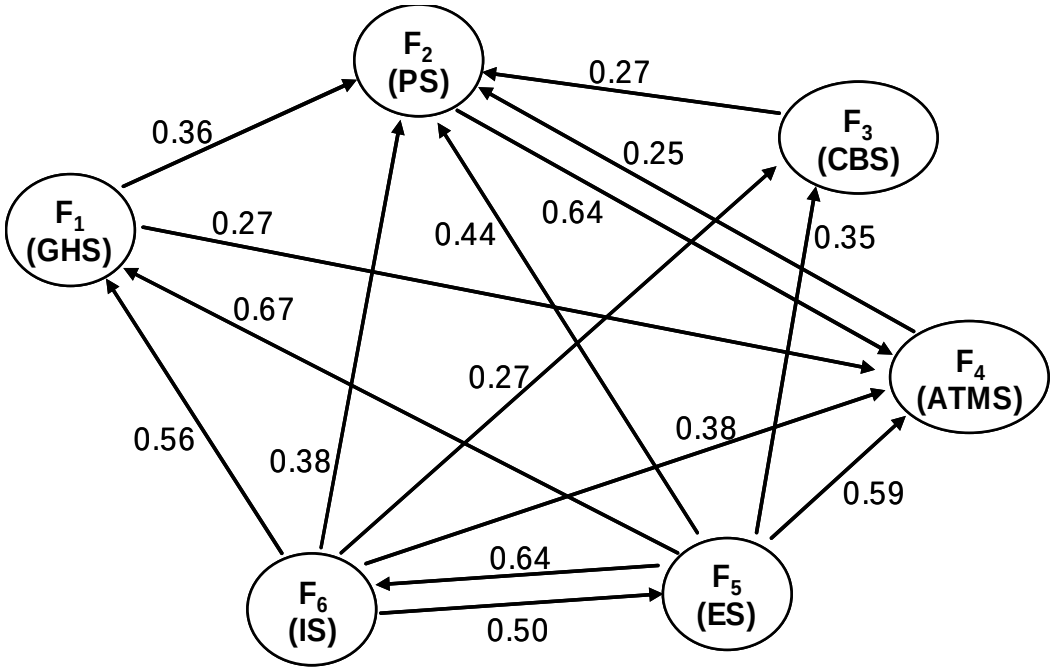


Figure 3.5: FCM model for airport X.

Step 9: The FCM model is simulated using Eq.3.16 and function vulnerability values reach an equilibrium state after a few iterations. The calculated function vulnerability values for 10 iterations are presented in Table 3.10 and equilibrium of concept values are shown in Figure 3.6.

Table 3.10: The vulnerability values of functions for 10 iterations.

Functions	Iterations									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
F_1	0.932	0.840	0.848	0.855	0.858	0.859	0.859	0.859	0.859	0.859
F_2	0.766	0.908	0.928	0.933	0.934	0.935	0.935	0.935	0.935	0.935
F_3	0.865	0.773	0.772	0.776	0.778	0.779	0.779	0.779	0.779	0.779
F_4	0.729	0.845	0.879	0.888	0.890	0.890	0.891	0.891	0.891	0.891
F_5	0.245	0.678	0.742	0.755	0.758	0.759	0.759	0.759	0.759	0.759
F_6	1.000	0.761	0.768	0.777	0.779	0.780	0.781	0.781	0.781	0.781

As seen from Table 3.10 and Figure 3.6, after the FCM simulation, PS function has become the most vulnerable function in the long run with a vulnerability value of $V_{F_2} = 0.935$. The reason is that, this function is affected by all the other functions. This means an increase in the vulnerability value of any function creates an increase in the vulnerability value of PS function. On the other hand, ES function has become relatively the least vulnerable function with $V_{F_5} = 0.759$ after the simulation as it is the least affected function in the system. The results in Table 3.10 also show that

after the FCM simulation the most influenced function has the highest vulnerability value; whereas the least influenced function has the lowest vulnerability value.

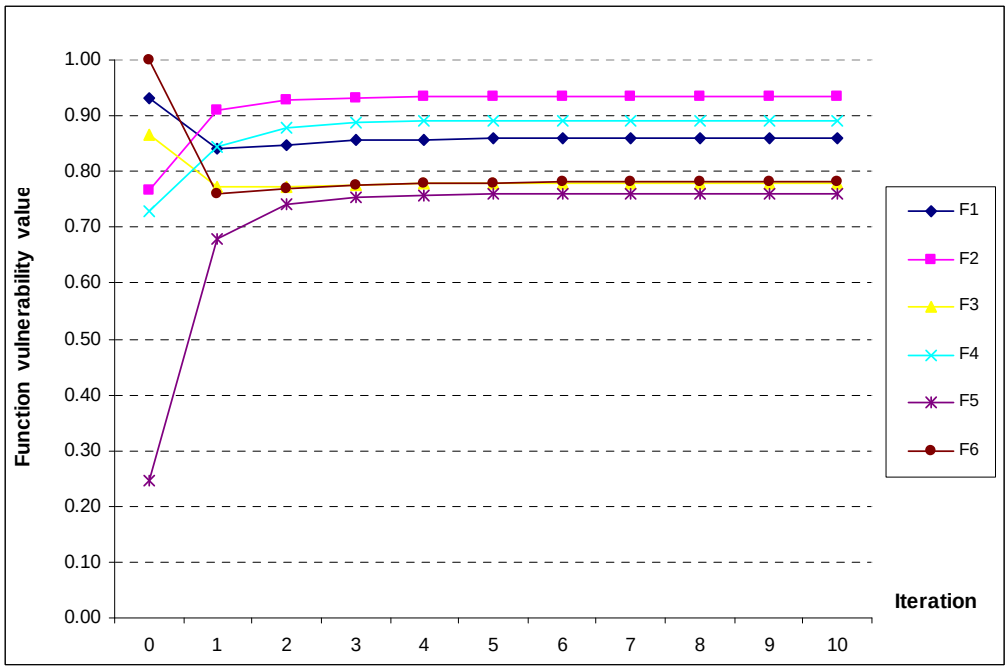


Figure 3.6: Equilibrium state of the function vulnerability values.

Step 10: The hidden and real vulnerability values of the components, functions and the system are calculated using Eqs.3.17-3.26 and shown in Table 3.11.

Step 11: The rankings and the vulnerability values before and after FCM simulation are presented in Table 3.11. It is observed that the ranks of functions and components are different due to the hidden vulnerabilities caused by the logical interdependencies among the functions. For instance, while IS function has the same rank before and after the simulation, ES functions has greatly different ranks. Although, this function has the least vulnerability before simulation, it becomes the second most vulnerable after simulation as it has the highest hidden vulnerability ($V_{F_5}^h = 2.293$). On the other hand, PS function becomes the least critical function of Airport X having the least real vulnerability value after simulation. It can be concluded that the IS function, with the real vulnerability of $V_{F_6} = 2.774$, is determined as the most critical function for Airport X.

At the component level, this rank difference is not as much as it is at the functional level. From Table 3.11, it is identified that “Power Centre Building” having the

highest real vulnerability of $V_{T_{62}} = 2.069$, is the most critical component for Airport X. This component also has the highest hidden vulnerability ($V^h_{T_{62}} = 1.069$). "Main Entrance and Security Control Building" has the least vulnerability ($V_{T_{51}} = 0.158$) and rank before the simulation, but its rank and criticality is increased by five after the simulation since it has the second highest hidden vulnerability ($V^h_{T_{51}} = 0.490$).

Table 3.11: Comparison of the vulnerability values.

	Before FCM simulation		**After FCM simulation**		**Hidden vulnerability**
	Vulnerability	**Rank**	**Vulnerability**	**Rank**	
System	0.749	-	1.621	-	0.872
Functions					
F_1	0.932	2	1.506	3	0.574
F_2	0.766	4	0.985	6	0.220
F_3	0.865	3	1.121	5	0.256
F_4	0.729	5	1.330	4	0.601
F_5	0.245	6	2.538	2	2.293
F_6	1.000	1	2.774	1	1.774
Components					
T_{11}	0.904	5	1.202	4	0.298
T_{12}	0.907	4	1.183	5	0.276
T_{21}	0.758	9	0.919	8	0.161
T_{22}	0.679	11	0.710	14	0.031
T_{23}	0.735	10	0.763	12	0.028
T_{31}	0.780	8	0.889	9	0.108
T_{32}	0.886	6	1.033	7	0.147
T_{41}	0.790	7	1.090	6	0.301
T_{42}	0.630	12	0.742	13	0.112
T_{43}	0.626	13	0.814	10	0.188
T_{51}	0.158	20	0.648	15	0.490
T_{52}	0.177	19	0.606	16	0.430
T_{53}	0.458	14	0.803	11	0.345
T_{54}	0.238	16	0.583	17	0.345
T_{55}	0.220	17	0.425	19	0.205
T_{56}	0.197	18	0.541	18	0.345
T_{57}	0.289	15	0.424	20	0.135
T_{61}	0.933	2	1.272	3	0.339
T_{62}	1.000	1	2.069	1	1.069
T_{63}	0.926	3	1.291	2	0.365

The high vulnerable or in other words most critical components of Airport X are the most probable possible targets for the terrorist attacks. Hence, the appropriate defence resource should be allocated in the following defence resource planning process to improve site security of Airport X.

Finally, the systematic application of the FIVAM satisfactorily contributes the overall vulnerability assessment process of Airport X. This approach can originally be utilized as a decision aid by the related managers; moreover, it provides both motivation and contributions on vulnerability assessment process as one of the critical administrative issue consistently.

3.6 Concluding Remarks of Chapter 3

In the last decade, the number of adversary attacks to the critical facilities has increased dramatically and SRA has gained more importance. Managing the risk of these facilities for the adversary attacks depends on systematic and quantitative vulnerability assessment.

Vulnerability assessment should be conducted at three levels: system level, system function level and system component level. Furthermore, the most critical functions and components in the system have to be determined and ranked to support the following defence resource planning process.

When the nature of this problem is analyzed, it seems that the fuzzy SMART and FCM integration, proposed FIVAM framework, can be recognized as a suitable research methodology towards the solution of this problem. FIVAM takes the advantages of the fuzzy SMART for determining the vulnerability of system under multiple qualitative/quantitative criteria in GDM environment, and FCM for modelling the behaviour of the system to monitor the vulnerability.

The case application of an example airport illustrates the utility and effectiveness of the proposed FIVAM framework. The quantitative findings on the case study highlight that possible interrelationships among the system functions are very significant in vulnerability assessment of a critical facility and they have to be taken into account in the system perspective. By doing this, hidden vulnerabilities can be identified consistently. That’s why; the FIVAM framework becomes more realistic and applicable to overcome this issue. Furthermore, FIVAM can be utilized as a simple and practical toolkit for this type of real life problems for enhancing the current procedures in vulnerability assessment process. To realize this idea, FIVAM can be applied similarly in some cases to assess the vulnerability of any other facilities that can be a metro station, shopping mall, metro station, harbour,

governmental facility, military bases, chemical plants, oil refinery etc. In addition to this, both the number of evaluation criteria and system components can be increased in order to conduct a detailed assessment at the operational and tactical level.

The further research can be performed on extending the FIVAM framework to assign defence resources for the most vulnerable components to comprehensively support this critical decision-making problem. For this purpose, SWOT analysis as a strategy-making tool can be integrated into the FIVAM framework for identifying and formulating appropriate counter-measure strategies in defence planning.

4. CONSEQUENCE ASSESSMENT MODELLING

4.1 Introduction to Consequence Assessment

In SRA, the objective of consequence assessment (CA) is to estimate the expected magnitudes and types of losses (e.g., deaths, injuries, or property damage) associated with a threat scenario given adversary success. CA is an important part of SRA because wrong CA leads to the wrong estimation of the security risk. The most important aspect of CA is the identification, quantification and integration of all different types of losses specific to security risk while estimating the total consequence of a critical facility.

In the literature, there are models that estimate the damage to a building based on the quantity of fire, explosion, and toxic release and dispersion. The CA schemes for chemical process industries are mainly common in the literature and they are based on the models of accidental fire, explosion, and toxic release and dispersion (Khan and Abbasi, 1998; 1999; 2000; Arunraj and Maiti, 2009). The existing models of accidental fire, explosion, and toxic release and dispersion are mainly based on either empirical methods or numerical methods (Remennikov, 2003). Empirical methods are analytical methods that are correlations with experimental data while numerical methods are computational fluid dynamics models that are based on mathematical equations of basic physic laws.

The available complex methodologies lacks in estimating the losses due to security risk consequences. Threat scenario as an initiating event causes explosions and fire or combinations of these main events leading to losses. Therefore, model estimating the effects of explosive blast on humans and structures due to size of explosions and fire is needed. Therefore, the consequence modelling for SRA has to be performed by considering all major losses of security risk with optimal complexity and optimal time to improve the SRA.

This chapter proposes the Monte Carlo Simulation based CA model (CAM) that combines different types of consequences for SRA. After reviewing the existing

approaches and the factors that influence the CA, the remainder of this chapter is organized as follows: In Section 4.2, theoretical background information for the proposed approach is represented. The proposed model and its process flow are introduced in Section 4.3. The illustrative application of the proposed approach is performed over an airport case study in Section 4.4. This section also examines the utility of findings and discusses the analysis results. Conclusions and further issues are addressed respectively in the final section.

4.2 Theoretical Background for Consequence Assessment Modelling

In this section, theoretical background information on Monte Carlo simulation (MCS) and Trinitrotoluene (TNT) equivalent method are presented, respectively.

4.2.1 Monte Carlo simulation

MCS is a complex stochastic problem technique used to solve a wide range of mathematical problems in numerous fields such as mathematics, physics and engineering (Rubinstein and Kroese, 2007). MCS is used to approximate the probability of certain outcomes by running multiple trials, called simulations, using random variables. The basic idea of MCS is as follows: MCS randomly selects values from given distributions for the defined random variables of the given problem. Then, it forms one possible solution to the problem for each trial. Finally, these trials give a range of possible solutions, resulting in a probability distribution for the outcome parameter. MCS is also called random sampling technique or statistical experimental approach.

In this study, MCS is used to calculate the consequence of given threat scenarios for CA.

4.2.2 TNT equivalent method

TNT equivalent method is a set of equations which relate the energy of explosion in terms of TNT equivalent weight, distance from explosion, and blast pressure in the literature (Cooper, 1996; Diaz Alonso et al., 2006; Diaz Alonso et al., 2007; Diaz Alonso et al., 2008; Usmani and Kirk, 2008; Usmani et al., 2009). TNT equivalent method is widely used empirical method and computationally simple for loss calculation. The experimental data show that when different amount of TNT

explodes, the shock wave overpressure produced can be calculated by the following scaling law of equation (Cooper, 1996):

$$\frac{R}{R_0} = \left(\frac{W_{TNT}}{W_0} \right)^{1/3}, \Delta P = \Delta P_0 \quad \textbf{(4.1)}$$

where R is the distance between target and explosion centre in meters (m), R_0 is the distance between target and reference explosion centre in m, W_0 is the reference TNT equivalent weight in kilograms (kg), W_{TNT} is the TNT equivalent weight of threat scenario in kg, ΔP is the overpressure at the target in MPa, and ΔP_0 is the overpressure at the reference target in mega pascal (MPa). Eq. 4.1 shows that ratio of the distance R to R_0 is equal to the cube root of the ratio of W_{TNT} to W_0 under the same overpressure.

The typical shock wave overpressure produced by reference explosion of 1000kg TNT is listed in Table 4.1 and the possible losses caused by shock wave overpressure are listed in Table 4.2 (Huang and Cheng, 2009). By using the experimental data like in Table 4.1 and in Table 4.2, R_0 and ΔP_0 in Eq. 4.1 can be determined by interpolation for all loss types.

Table 4.1 : The shock wave overpressure of W_0=1000kg TNT explosion.

Distance R_0 (m)	Overpressure ΔP_0 (10^5MPa)	Distance R_0 (m)	Overpressure ΔP_0 (10^5MPa)
5	30	25	0.81
6	21	30	0.59
7	17	35	0.44
8	13	40	0.34
9	9.7	45	0.28
10	7.8	50	0.24
12	5.1	55	0.21
14	3.4	60	0.184
16	2.4	65	0.164
18	1.74	70	0.146
20	1.29	75	0.132

In this study, TNT equivalent method is used to describe the energy of threat scenario by converting the weapon type and magnitude of threat scenario to the amount of TNT that releases the same amount of energy and then using the experimental data related to TNT explosion effect to predict the effect of threat scenario.

Table 4.2 : Possible losses caused by shock wave overpressure.

Overpressure ΔP_0 (10^5MPa)	Losses
0.05 ~ 0.06	Part of glasses of door and window broken
0.06 ~ 0.10	Most of pressurized glasses of door and window broken
0.15 ~ 0.20	Window frame damaged
0.20 ~ 0.30	Wall cracked, slight injury of personnel
0.40 ~ 0.50	Big cracks in wall, tiles falling off, intermediate injury of personnel
0.60 ~ 0.70	Column of wooden buildings broken, building frame loose, serious injury or death of personnel
0.70 ~ 1.00	Brick wall collapsed, serious injury or death of personnel
1.00 ~ 2.00	Vibration-proof reinforced concrete damaged, small house collapsed, most personnel dead
2.00 ~ 3.00	Large steel structure damaged, majority of personnel dead

4.3 Monte Carlo Simulation based Consequence Assessment Model

Given a threat scenario, there are three main challenges in CA: identification, estimation and aggregation of consequence dimensions. For identification of consequence dimensions, literature is reviewed and the types of losses are classified for security risk of a critical facility (Khan and Haddara, 2004). Since the consequence from a threat scenario is multidimensional, the proposed model examines three main consequence dimensions (Figure 4.1). Additional or fewer dimensions can also be considered. The definitions of identified consequence dimensions are as follows:

- Assets loss (AL): This loss is the loss due to the occurrence of both equipment damage and building damage resulted from a given threat scenario.
- Human loss (HL): This loss is the loss due to the occurrence of fatalities and/or injuries resulted from a given threat scenario.
- Operational loss (OL): This loss is the loss due to the occurrence of profit loss from downtime resulted from a given threat scenario.

For estimation of consequence dimensions, TNT equivalent method described in Section 4.2.2 is applied for the transformation of a threat scenario into corresponding consequence. TNT equivalent method is applied to CA for AL, HL and OL calculations in this study.

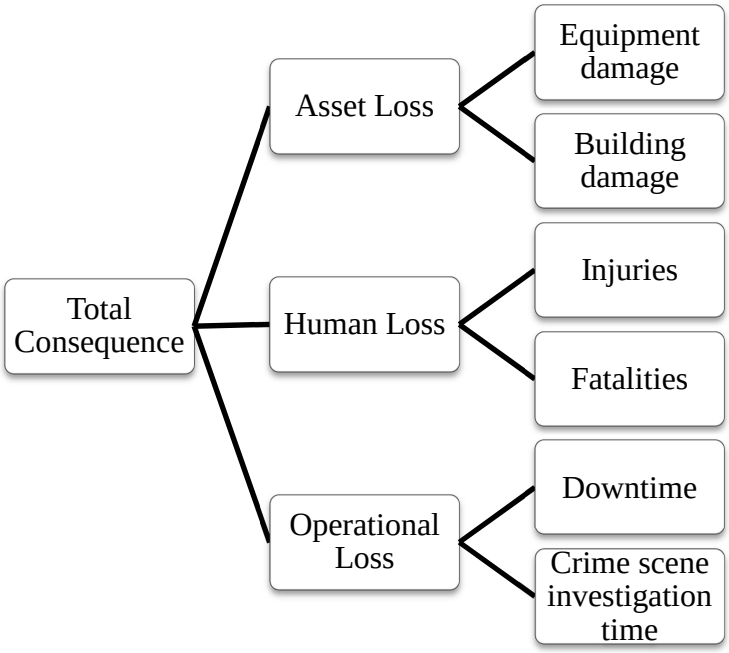


Figure 4.1 : The consequence dimensions.

For comparison and aggregation of consequence dimensions, a single measure of total consequence is required. The loss is assessed for each consequence dimension with different unit of measure. A single measure of total loss can be obtained through converting losses from their natural units to a dimension that facilitates comparison and aggregation. There are different consequence measures in the literature. Many of the consequence measures focus on financial loss. Therefore, in this study all the consequence dimensions are measured in monetary terms. The asset loss is measured in Liras (L) to repair or replace the damaged equipment and building. Although the value of life is immeasurable and there is a discomfort associated with monetary valuation of human life, this loss is calculated in terms of number of fatalities and/or injuries times the life insurance cost and/or rehabilitation costs. Different rehabilitation costs are also considered since the rehabilitation costs for injuries vary according to the severity of the injury. The operational loss is measured in Liras (L) due to profit loss to resume critical facility functionality. As a result, all the consequence types are expressed in units of cost (L) per consequence dimension, and this provides a measure of the loss given the occurrence of a specific threat scenario.

In the estimation of the total consequence, stochastic nature of the input parameters is taken into consideration. Data relating to all consequence types in security risk is collected from the existing scientific literature for a critical facility. The input

parameters for all types of losses to which an exact value can not be assigned are determined and described with probability distributions. These parameters are modelled as a random variable which accepts specific probability distribution function. Values for the random variables in CAM are determined by MCS. Detailed descriptions of the input parameters are discussed and tables of model inputs and distributions are provided in following sub-sections. After defining the parameters and their probabilistic behaviours, total consequence is estimated with respect to these parameters by using MCS and TNT equivalent method for a critical facility.

The proposed approach consists of the following steps shown in Figure 4.2.

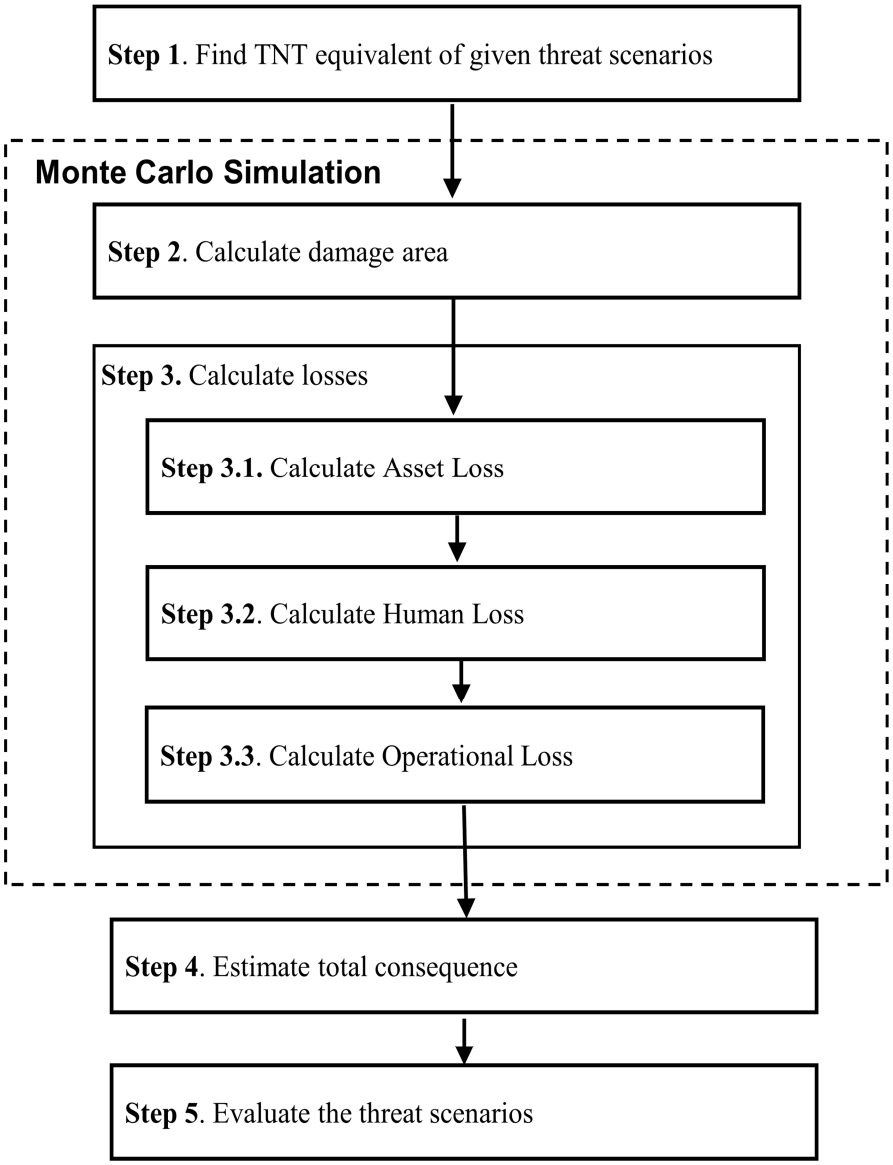


Figure 4.2 : Steps of proposed approach.

Step 1: Find TNT equivalent

TNT equivalent weight of threat scenario is determined by weapon type and magnitude of a given scenario. MCS is used to generate random numbers following determined distribution for TNT weight based on weapon type and magnitude of given threat scenario from both historical data and technical data of weapon type.

$W_{TNTi} = f(\text{weapon type}_i, \text{magnitude}_i)$ **(4.2)**

where W_{TNTi} is the TNT equivalent weight of scenario i in kg based on weapon type and magnitude of threat scenario i.

Step 2: Calculate damage radius

Damage radiuses are used to quantify the determined types of losses. Different damage radiuses are calculated for all different types of losses based on TNT equivalent of a given threat scenario. The damage radiuses are computed by using the scaling law of equation as follows:

$$\frac{R_k}{R_0} = \left(\frac{W_{TNTi}}{W_0} \right)^{1/3}, \Delta P = \Delta P_0 \quad \textbf{(4.3)}$$

where R_k is the radius (m) of type k loss given R_0, W_0 and ΔP_0. R_0 is the distance between target and reference explosion centre in m, W_0 is the reference TNT equivalent weight in kg, W_{TNTi} is the TNT equivalent weight of threat scenario i in kg, ΔP is the overpressure at the target in MPa, ΔP_0 is the overpressure at the reference target in MPa, and k is the type of loss {Equipment Damage (ED), Building Damage (BD), Fatality (Fat), Serious Injury (SeI), Slight Injury (SlI)}.

Step 3: Calculate losses

The calculated damage radiuses are used to compute the effects on assets, humans, and operations. It is assumed that physical objects like walls, furniture etc. in the buildings and blockage effect of human to human do not provide protection as obstacles/shields or do not cause extra harm.

Step 3.1: Calculate asset loss

Asset loss involves both equipment damage and building damage. Therefore, asset loss is calculated as in the following sub-steps.

Step 3.1.1: Calculate equipment damage cost

Equipment damage is formulated as follows:

$EDC_i = \pi R_{ED}^2 * ED_{ij}$ **(4.4)**

where EDC_i is the equipment damage cost (L) of threat scenario i, R_{ED} is the equipment damage radius (m), ED_{ij} is the equipment density in the vicinity of the jth part of target related to threat scenario i (L/m^2) and j is the part of the target {perimeter, protected areas, infrastructure systems}.

Step 3.1.2: Calculate building damage cost

Building damage is formulated as follows:

$$BDC_i = \frac{\pi R_{BD}^2}{BA_i} * BC_i \quad \textbf{(4.5)}$$

where BDC_i is the building damage cost (L) of threat scenario i, R_{BD} is the building damage radius (m), BA_i is the total area of target building related to threat scenario i (m^2) and BC_i is the value of the target building related to threat scenario i (L).

After equipment damage cost (EDC_i) and building damage cost (BDC_i) are calculated, asset loss is computed by using the following formula:

$AL_i = EDC_i + BDC_i$ **(4.6)**

where AL_i is asset loss of the threat scenario i.

Step 3.2: Calculate human loss

Human loss involves both fatalities and injuries. Injuries can be either serious injury or slight injury. Therefore, human loss is calculated as in the following sub-steps.

Step 3.2.1: Calculate fatality cost

Fatality cost is formulated as follows:

$$FC_i = \frac{\pi R_{Fat}^2}{10,000 m^2} * HD_{ij} * HFC \quad \textbf{(4.7)}$$

where FC_i is the fatality cost (L/person) of threat scenario i, R_{Fat} is the fatality radius (m), HD_{ij} is the human population density in the vicinity of the jth part of target related to threat scenario i (person/hectare(ha)), HFC is the cost of one fatality and j is the part of the target {perimeter, protected areas, infrastructure systems}. Note that

damage area is calculated in m^2 and than converted to ha by dividing the damage area to 10,000m^2 since 1ha is equal to 10,000m^2.

Step 3.2.2: Calculate serious injury cost

Serious injury cost is formulated as follows:

$$SeIC_i = \frac{\pi R_{SeI}^2}{10,000m^2} * HD_{ij} * SeC \quad \textbf{(4.8)}$$

where $SeIC_i$ is the serious injury cost (L/person) of threat scenario i, R_{SeI} is the serious injury radius (m), HD_{ij} is the human population density in the vicinity of the jth part of target related to threat scenario i (person/ha), SeC is the serious injury cost and j is the part of the target {perimeter, protected areas, infrastructure systems}.

Step 3.2.3: Calculate slight injury cost

Slight injury cost is formulated as follows:

$$SlIC_i = \frac{\pi R_{SlI}^2}{10,000m^2} * HD_{ij} * SlC \quad \textbf{(4.9)}$$

where $SlIC_i$ is the slight injury cost (L/person) of threat scenario i, R_{SlI} is the slight injury radius (m), HD_{ij} is the human population density in the vicinity of the jth part of target related to threat scenario i (person/ha), SlC is the slight injury cost and j is the part of the target {perimeter, protected areas, infrastructure systems}.

After fatality cost (FC_i), serious injury cost ($SeIC_i$) and slight injury cost ($SlIC_i$) are calculated, human loss is computed by using the following formula:

$$HL_i = FC_i + SeIC_i + SlIC_i \quad \textbf{(4.10)}$$

where HL_i is human loss of the threat scenario i.

Step 3.3: Calculate operational loss

OL is estimated using the following relation:

$$t_d = \max(t_{ERecover}, t_{BRecover}, t_{CSI}) \quad \textbf{(4.11)}$$

where t_d is the time spent for repairs or downtime (hour), $t_{ERcover}$ is the speed of time for replacement and reinstallation of damaged equipments (hour/damage ratio), $t_{BRecover}$ is the speed of time for reconstruction of damaged building (hour/damage

ratio), and t_{CSI} is the speed of time for crime scene inspection (hour/damage ratio). Note that damage ratio is a proportion of damage area to building area.

$$OL_i = OuC * t_d \quad \textbf{(4.12)}$$

where OL_i is the operational loss of threat scenario i (L) and OuC is the service/production value per hour (L/hour).

Step 4: Estimate total consequence

Total consequence is formulated as follows:

$$TC_i = AL_i + HL_i + OL_i \quad \textbf{(4.13)}$$

where TC_i is the total consequence, AL_i is the asset loss, HL_i is the human loss and OL_i is the operational loss of threat scenario i.

Step 5: Evaluate the threat scenarios

At this step, the threat scenarios are ranked and compared based on their total consequences. Furthermore, CA is presented and discussed.

4.4 An illustrative example for Consequence Assessment

In this section, the proposed model as described in Section 4.3 is applied to the CA of a hypothetical Airport X. Possible threat scenarios identified in Chapter 2 are used for CA (Table 2.11). Note that for security reasons, all the data used throughout this example are purely generic and notional. Even though this case study is very simple, the resulting qualitative relationships and insights drawn from this example validate the proposed approach. A step-by-step algorithm for this example is as follows:

Step 1: Find TNT equivalent

TNT equivalent weight of threat scenario is determined by weapon type and magnitude of a given scenario. Both historical data and technical data of weapon type are reviewed in the unclassified literature. It is seen that: Large trucks typically contain 11,340 kilograms or more of TNT equivalent, and vans typically contain 2,268 to 11,340 kilograms. Small automobiles can contain 23 to 2,268 kilograms of TNT equivalent. A briefcase bomb is about 23 kilograms, and a suicide bomber wearing a vest belt generally carries up to 14 kilograms of TNT equivalent (Usmani and Kirk, 2008). It is assumed that TNT equivalent weight of weapon type-

magnitude pairs follows triangular distribution. Therefore, minimum, most likely and maximum ranges of TNT weight in kg for threat scenarios are given in the Table 4.3.

MCS generates random numbers following triangular distribution with given parameters for TNT weight based on weapon type and magnitude.

Table 4.3 :TNT Equivalent weights.

Weapon Type and Magnitude	TNT equivalent weight (kg)		
	Minimum	Most Likely	Maximum
Explosives-Low (a_1^2, a_1^4)	5	9	13
Explosives-Medium (a_1^2, a_2^4)	14	18	22
Truck/Car bomb-Low (a_2^2, a_1^4)	31	1,150	2,267
Truck/Car bomb-Medium (a_2^2, a_2^4)	2,268	6,804	11,339

Step 2: Calculate damage radius

By using Table 4.1 and Table 4.2, R_0 and ΔP_0 in Eq. 4.3 are determined by interpolation for all loss types.

Step 2.1: Calculate asset loss radius

Step 2.1.1: Calculate equipment damage radius

By using Table 4.1 and Table 4.2, ΔP_0 and R_0 are determined by interpolation for equipment damage as ΔP_0=0.2MPa and R_0=56.9m respectively. Therefore, equipment damage radius (R_{ED}) is calculated based on Eq. 4.3 as follows:

$$\frac{R_{ED}}{56.9} = \left(\frac{W_{TNT}}{1000}\right)^{1/3}, \Delta P = 0.2\,\text{MPa} \qquad \textbf{(4.14)}$$

Step 2.1.2: Calculate building damage radius

As airports are generally constructed as either reinforced concrete structures or large steel structures, the shockwave pressure value at which these structures are damaged is used. According to Table 4.1 and Table 4.2, ΔP_0 and R_0 are determined by interpolation for building damage as ΔP_0=2MPa and R_0=17.2m respectively. Therefore, building damage radius (R_{BD}) is calculated based on Eq. 4.3 as follows:

$$\frac{R_{BD}}{17.2} = \left(\frac{W_{TNT}}{1000}\right)^{1/3}, \Delta P = 2\,\text{MPa} \qquad \textbf{(4.15)}$$

Step 2.2: Calculate human loss radius

Step 2.2.1: Calculate fatality radius

By using Table 4.1 and Table 4.2, ΔP_0 and R_0 are determined by interpolation for fatality as ΔP_0=0.6MPa and R_0=30m respectively. Therefore, fatality radius (R_{Fat}) is calculated based on Eq. 4.3 as follows:

$$\frac{R_{Fat}}{30} = \left(\frac{W_{TNT}}{1000}\right)^{1/3}, \Delta P = 0.6\,\text{MPa} \quad \textbf{(4.16)}$$

Step 2.2.2: Calculate serious injury radius

By using Table 4.1 and Table 4.2, ΔP_0 and R_0 are determined by interpolation for serious injury as ΔP_0=0.3MPa and R_0=44m respectively. Therefore, equipment serious injury radius (R_{SeI}) is calculated based on Eq. 4.3 as follows:

$$\frac{R_{SeI}}{44} = \left(\frac{W_{TNT}}{1000}\right)^{1/3}, \Delta P = 0.3\,\text{MPa} \quad \textbf{(4.17)}$$

Step 2.2.3: Calculate slight injury radius

By using Table 4.1 and Table 4.2, ΔP_0 and R_0 are determined by interpolation for slight injury as ΔP_0=0.138MPa and R_0=72.1m respectively. Therefore, slight injury radius (R_{SlI}) is calculated based on Eq. 4.3 as follows:

$$\frac{R_{SlI}}{72.1} = \left(\frac{W_{TNT}}{1000}\right)^{1/3}, \Delta P = 0.138\,\text{MPa} \quad \textbf{(4.18)}$$

Step 3: Calculate Losses

Step 3.1: Calculate Asset Loss

Step 3.1.1: Calculate equipment damage cost

All the equipments of Airport X are assumed as though they were uniformly distributed over the entire unit area in this study. Airport X parameters for equipment damage are given in the Table 4.4 and equipment damage cost is calculated for a threat scenario i by using Eq. 4.4.

Table 4.4 : Airport X parameters for equipment damage.

Target i	Equipment Density (ED_{ij}), L/ m^2		Equipment Cost (EC_i), L
	Perimeter	Protected Areas	
a_3^1 Passenger Terminal	200	600	113,400,000
a_4^1 Parking Facility	5	250	25,075,000
a_5^1 Bus Station	10	100	253,750
a_{11}^1 Main Entrance and Security Control Building	90	200	256,200

Step 3.1.2: Calculate building damage

Airport X parameters for building damage are given in the Table 4.5 and building damage cost is calculated for a threat scenario i by using Eq. 4.5.

Table 4.5 : Airport X parameters for building damage .

Target i	Building Area (BA_i), m^2	Building Peripheral Area (BPA_i), m^2	Total Building Cost (TBC_i), L	Building Unit Cost (BC_i), L/m^2
a_3^1 Passenger Terminal	180,000	207,000	222,300,000	1,235
a_4^1 Parking Facility	100,000	115,000	15,000,000	150
a_5^1 Bus Station	2,500	2,875	1,752,500	701
a_{11}^1 Main Entrance and Security Control Building	1,200	1,380	356,400	297

Step 3.2: Calculate Human Loss

Airport X parameters for human loss are determined reasonably by using historical data and given in the Table 4.6 and Table 4.7 (SAA, 2009; Turkstat 2009).

Table 4.6 : Airport X parameters for human density of human loss.

Target i	Human Density (HD_i), persons/ha	
	Perimeter	Protected Areas
a_3^1 Passenger Terminal	1000	3500
a_4^1 Parking Facility	15	25
a_5^1 Bus Station	500	2000
a_{11}^1 Main Entrance and Security Control Building	250	1500

Different rehabilitation costs are also considered since the rehabilitation costs for injuries vary according to the severity of the injury. It is assumed that injury costs

follow triangular distributions. Therefore, minimum, most likely and maximum ranges of cost (L) for injury types are given in the Table 4.7.

Table 4.7 : Airport X parameters for injury types of human loss .

Injury	Min	Most Likely	Max
Fatality cost	-	50,000	-
Serious Injury cost	11,000	25,500	40,000
Slight Injury cost	1,000	5,500	10,000

Fatality cost, serious injury cost, slight injury cost and human loss is calculated for a threat scenario i by using Eq. 4.7-4.10.

Step 3.3: Calculate Operational Loss

Airport X parameters for operational loss are given in the Table 4.8 and operational loss for threat sceanrio i is calculated for a threat scenario i by using Eq. 4.11.

In this study, it is assumed that operational loss category speeds follows triangular distribution. Minimum, most likely and maximum ranges of time (hours) for operational loss categories are given in the Table 4.8. The service value per hour (OuC) is taken 270,000L/hour.

Table 4.8 : Airport X parameters for operational loss .

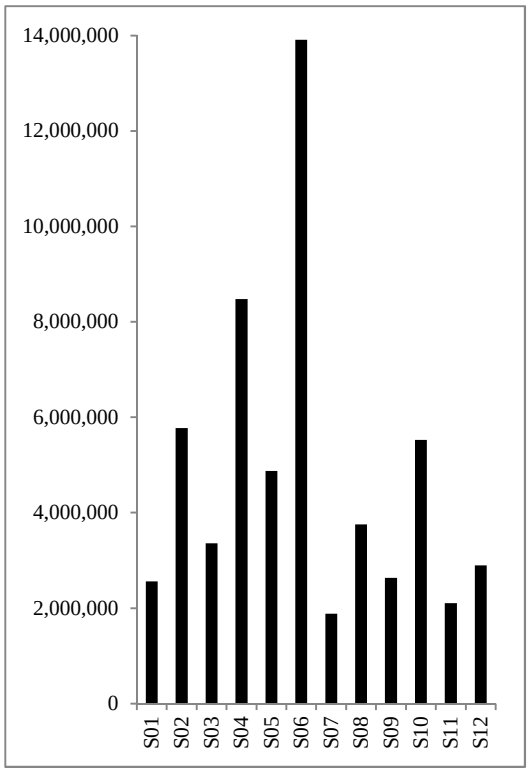
Speed (hour)	Damage ratio<33%			33%≤Damage ratio≤66%			66%<Damage ratio		
	Min	Most Likely	Max	Min	Most Likely	Max	Min	Most Likely	Max
Equipment Recovery speed (t_{ER})	1	3	5	3	5	8	5	8	12
Building Recovery speed (t_{BR})	2	4	6	5	8	10	8	10	12
CSI speed (t_{CSI})	2	4	6	4	6	8	6	8	12

Step 4: Estimate total consequence

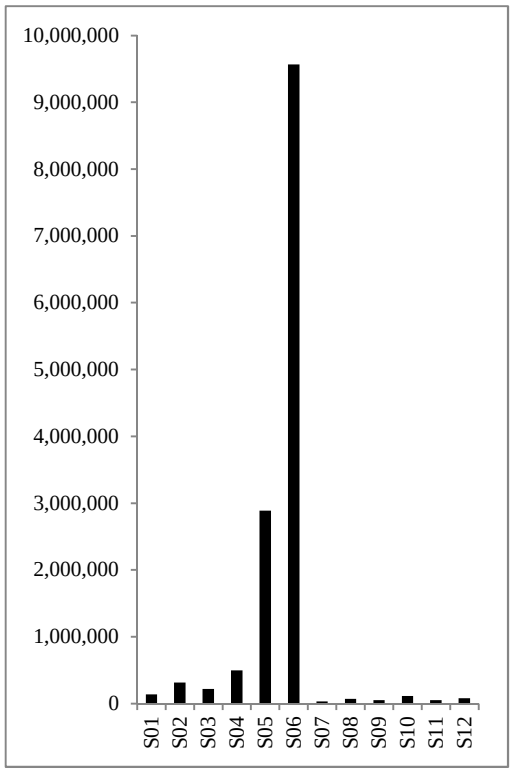
The model is developed in Microsoft Excel. The model is run for 500 iterations using Monte Carlo sampling. The model is performed using the parameters and calculations presented. The model simulates the all consequence types for the given threat scenario. The simulated minimum, maximum and mean values of total consequence and all the loss types are calculated. The results of overall consequence calculation are shown in Table 4.9 and Figure 4.3.

Table 4.9 : Simulation results.

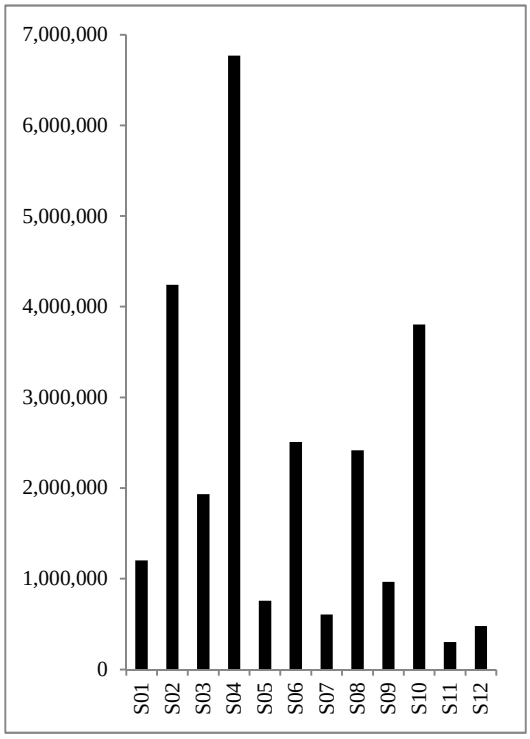
	Total Consequence (L)			Asset Loss (L)			Human Loss (L)			Operational Loss (L)		
Threat Scenario	**Min**	**Mean**	**Max**	**Min**	**Mean**	**Max**	**Min**	**Mean**	**Max**	**Min**	**Mean**	**Max**
1 $(a_3^1, a_1^2, a_1^3, a_1^4)$	1,855,044	2,557,497	3,306,729	95,416	136,179	171,383	736,642	1,203,190	1,735,559	707,918	1,218,129	1,607,319
2 $(a_3^1, a_1^2, a_2^3, a_1^4)$	4,114,586	5,776,055	7,920,885	218,557	312,922	395,561	2,535,876	4,240,495	6,430,380	727,513	1,222,638	1,601,086
3 $(a_3^1, a_1^2, a_1^3, a_2^4)$	2,601,305	3,360,789	4,176,256	186,769	218,373	247,723	1,223,938	1,934,325	2,497,974	683,784	1,208,091	1,587,441
4 $(a_3^1, a_1^2, a_2^3, a_2^4)$	6,091,308	8,477,618	10,877,330	425,979	497,807	565,492	4,742,648	6,769,266	9,189,841	683,969	1,210,544	1,613,639
5 $(a_4^1, a_2^2, a_2^3, a_1^4)$	2,048,342	4,871,782	7,350,824	631,447	2,888,314	4,548,318	161,160	756,807	1,340,322	757,047	1,226,662	1,614,403
6 $(a_4^1, a_2^2, a_2^3, a_2^4)$	7,406,773	13,913,540	19,595,160	5,088,904	9,569,270	13,376,230	1,154,807	2,509,098	3,965,474	822,482	1,835,176	3,107,361
7 $(a_5^1, a_1^2, a_1^3, a_1^4)$	1,274,131	1,879,900	2,838,691	23,045	32,182	41,329	374,382	605,091	908,647	711,069	1,242,627	1,907,523
8 $(a_5^1, a_1^2, a_2^3, a_1^4)$	2,685,732	3,755,768	5,321,711	52,413	72,362	91,398	1,530,236	2,418,364	3,458,504	738,661	1,265,042	2,058,488
9 $(a_5^1, a_1^2, a_1^3, a_2^4)$	2,021,381	2,632,710	3,338,911	44,199	51,678	58,857	689,978	964,269	1,302,507	1,111,675	1,616,762	2,118,398
10 $(a_5^1, a_1^2, a_2^3, a_2^4)$	4,208,345	5,526,108	7,031,545	97,564	114,103	130,115	2,657,464	3,802,663	4,994,112	1,089,563	1,609,342	2,157,968
11 $(a_{11}^1, a_1^2, a_1^3, a_1^4)$	1,471,245	2,105,731	3,667,204	35,527	51,424	65,422	180,743	301,508	439,273	1,112,241	1,752,799	3,192,101
12 $(a_{11}^1, a_1^2, a_1^3, a_2^4)$	2,175,763	2,899,042	3,769,009	70,223	81,181	93,122	321,500	477,262	614,628	1,646,463	2,340,600	3,121,380



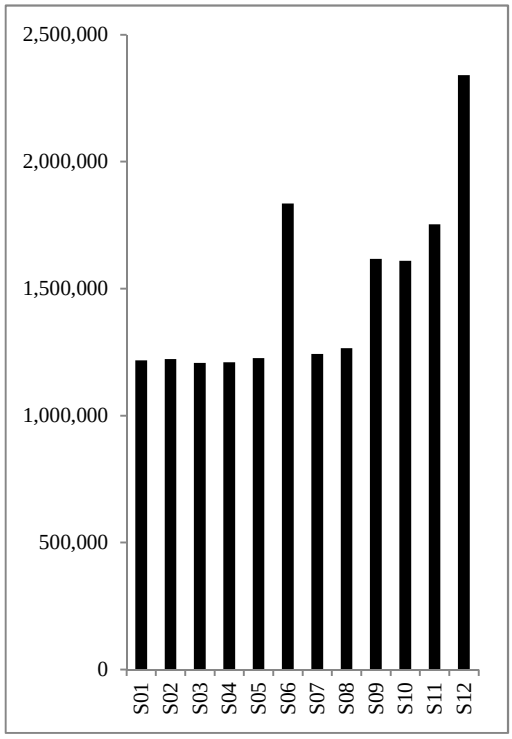
Total Consequence (L)



Asset Loss (L)



Human Loss (L)



Operational Loss (L)

Figure 4.3 : Histograms of simulation results.

Step 5: Evaluate the threat scenarios

The model resulted in a number of output distributions that can be used to predict the minimum, maximum and mean values of all consequence types given in Table 4.9. Rankings of consequences (total consequence, asset loss, human loss and operational loss) for threat scenarios are shown in Table 4.10. Rankings enable the DMs to identify the higher consequence scenarios from the lower consequence ones.

As seen from Table 4.9 and Figure 4.3, after the MCS, threat scenario 6 has the highest total consequnece with a total consequence value of 13,913,540 L and threat scenario 7 has the lowest total consequnece with a total consequence value of 1,879,900 L. From the MCS results, it is observed that targets with higher equipment density have higher asset loss and targets with higher human density have higher human loss. The results are useful to determine the precautions such as architectural and geometric changes of a critical facility considering both equipment density and human density for reducing asset loss, human loss, and operational loss. In addition, all the consequence types can also be evaluated on the basis of targets, parts of target attacked and weapon type-magnitude pairs.

Table 4.10 : Ranking of the simulation results.

Threat Scenario	Total Consequence		Asset Loss		Human Loss		Operational Loss	
	Mean (L)	Rank	Mean (L)	Rank	Mean (L)	Rank	Mean (L)	Rank
1 $(a_3^1, a_1^2, a_1^3, a_1^4)$	2,557,497	10	136,179	6	1,203,190	7	1,218,129	10
2 $(a_3^1, a_1^2, a_2^3, a_1^4)$	5,776,055	3	312,922	4	4,240,495	2	1,222,638	9
3 $(a_3^1, a_1^2, a_1^3, a_2^4)$	3,360,789	7	218,373	5	1,934,325	6	1,208,091	**12**
4 $(a_3^1, a_1^2, a_2^3, a_2^4)$	8,477,618	2	497,807	3	6,769,266	**1**	1,210,544	11
5 $(a_4^1, a_2^2, a_2^3, a_1^4)$	4,871,782	5	2,888,314	2	756,807	9	1,226,662	8
6 $(a_4^1, a_2^2, a_2^3, a_2^4)$	13,913,540	**1**	9,569,270	**1**	2,509,098	4	1,835,176	2
7 $(a_5^1, a_1^2, a_1^3, a_1^4)$	1,879,900	**12**	32,182	**12**	605,091	10	1,242,627	7
8 $(a_5^1, a_1^2, a_2^3, a_1^4)$	3,755,768	6	72,362	9	2,418,364	5	1,265,042	6
9 $(a_5^1, a_1^2, a_1^3, a_2^4)$	2,632,710	9	51,678	10	964,269	8	1,616,762	4
10 $(a_5^1, a_1^2, a_2^3, a_2^4)$	5,526,108	4	114,103	7	3,802,663	3	1,609,342	5
11 $(a_{11}^1, a_1^2, a_1^3, a_1^4)$	2,105,731	11	51,424	11	301,508	**12**	1,752,799	3
12 $(a_{11}^1, a_1^2, a_1^3, a_2^4)$	2,899,042	8	81,181	8	477,262	11	2,340,600	**1**

The case study results are compared with the similar past events such as the 2011 Domodedovo International Airport/Moscow bombing and the 2003 Brtitish

Consulate/Istanbul truck bomb attack for validation and verification. It is observed that result are reasonable.

4.5 Concluding Remarks of Chapter 4

CA is an important part of SRA because wrong CA leads to the wrong estimation of the security risk. Therefore, the main goal of this chapter is to develop a model that identifies, quantifies and integrates major types of losses specific to security risk while estimating the total consequence of a critical facility. For this purpose, Monte Carlo simulation based consequence assessment model using TNT equivalent method is proposed and complete logical model for CA is constructed in this study.

Firstly, CA schemes for different process industries suggested by various authors applicable to SRA are reviewed and CA model that can quantify impacts from identified threat scenarios for SRA is examined. The available complex methodologies lacks in estimating the losses due to security risk consequences and CA is required to be done with less calculation complexity by reducing efforts and time in SRA. Then, for identification of consequence dimensions, literature is reviewed and the types of losses are classified for security risk of a critical facility. Since the consequence from a threat scenario is multidimensional, the proposed model examines three main consequence dimensions, AL, HL and OL. Different from existing studies, CSI time is also considered for operational loss specific to SRA. Secondly, for estimation of consequence dimensions, TNT equivalent method integrated with MCS is applied for the transformation of a threat scenario into corresponding consequence. TNT equivalent method is applied to CA for AL, HL and OL calculations in this study.

To summarize, the proposed CA model identifies, quantifies and integrates all different types of losses specific to security risk of a threat scenario while estimating the total consequence. The proposed model performs CA by considering all major losses of security risk with optimal complexity and time to improve the SRA.

Although the main objective of the proposed model is CA, by using real data, the results of CAM can be used to determine the precautions such as architectural and geometric changes of a critical facility for reducing AL, HL, and OL. The correlation

between AL and equipment density, the correlation between HL and human density, and the correlations between all types of loss and building areas can also be explored.

In this study, total consequence is calculated by summing three equally weighted consequence type costs (Eq. 4.13). By changing the weights on the three consequence types (AL, HL, and OL), sensitivity analysis can be applied easily. If a greater proportion of the weight is allocated to the OL, this results in an increase in the OL cost of scenarios with operational assets such as air traffic control centre of an airport due to increased emphasis on service value of equipments. If a greater proportion of the weight is allocated to HL, this results in an increase in the HL cost of scenarios with heavily populated facilities such as passenger terminal of an airport.

Finally, as an illustration, the proposed model is applied to a case study. According to the results of CAM, suggestions for a critical facility protection can be put forward to reduce the losses. CAM enables security analyzers to identify the higher consequence scenarios from the lower consequence ones. Proposed model helps to improve SRA.

5. SECURITY RISK EVALUATION

5.1 Introduction to Security Risk Evaluation

The main objective of proposed SRA framework is to evaluate the security risk of a critical facility. This model of proposed SRA framework, security risk evaluation model (REM), involves determining the security risk priorities of a critical facility by quantifying the security risk.

Till now, a structured set of scenarios, their likelihoods, vulnerabilities and consequences have been quantified with different modes of uncertainty since security risk is measured in terms of threat likelihood (T), vulnerability (V), and consequence (C). In order to make correct decisions on the basis of the scenarios, T, V and C, the next thing is to properly aggregate them for evaluating the security risk. So, in this chapter, the key problem is to integrate T, V, and C to quantify the security risk. The choice of aggregation operators is crucial to the behaviour of the proposed SRA framework output. Therefore, aggregation operator is one of the basic brick of the proposed SRA framework.

Traditional methods require humans to translate their perceptions into numerical scales, frequently through mechanisms like a Likert scale. Following typical scoring method can be applied to security risk as qualitative SRA method. As security risk is a function of T, V, and C, one way to calculate it is to quantitatively assess T, V, and C, multiply the three factors to obtain a risk score, and make comparisons based on this risk score for a threat scenario. The risk score provides a quantitative measure of security risk associated with a threat scenario. For example, let the three factors T, V and C are all evaluated using the ratings (scores) from 1 to 5 as described in Table 5.1.

Table 5.1 : Ratings of security risk factors.

Qualitative definition			Quantitative definition
Threat Likelihood	Vulnerability	Consequence	(Score)
Extremely Likely	Very High	Catastrophic	5
Very Highly Likely	High	Major	4
Highly Likely	Medium	Very serious	3
Very Likely	Low	Serious	2
Likely	Very Low	Minor	1

Problems about typical security risk scoring method using multiplicative aggregation are as follows:

- Different sets of T, V and C ratings may produce exactly the same value of security risk score, but their hidden risk implications may be totally different. For example, two different threat scenarios with values of 1, 2, 6 and 6, 2, 1 for T, V and C respectively, will have the same security risk score value of 12. High likelihood-low consequence and low likelihood-high consequence threat scenarios can not be distinguished (limited resolution) since they may have same risk score.

- Small variations in one rating may lead to vastly different effects on the security risk score depending on the values of the other factors. For example, if T and V are both 5, then a 1 point difference in C rating results in a 25 point difference in the security risk score. If T and V are equal to 1, then the same 1 point difference results in only a 1 point difference in the security risk score. This is valid for all combinations of T, V and C.

- These factors are difficult to quantify and can not be adequately described numerically. For example, when security risk parameter is considered, the appropriate numeric scale for security risk is not known, does it range from 0 to 1, 1 to 10, or -10 to 10? If arbitrary numeric scales are used, the problem increases when factors are combined and the resultant numeric answer can not be understood.

As a result, multiplication is not the right aggregation operator and security risk factors must be aggregated in a nonlinear rather than linear manner.

The input information for REM in SRA framework comes from three different models: Threat Assessment Model (TAM), Vulnerability Assessment Model (VAM), and Consequence Assessment Model (CAM) that quantify T, V and C respectively as

shown in Figure 1.3 and Figure 1.4. Since each factor and corresponding proposed model has different uncertainty model, the other problem is how these three modes of representation of parameter uncertainty can be integrated for evaluating the security risk. Therefore, different formats of available data and uncertain knowledge must also be incorporated into SRA process.

This chapter proposes rule-based expert system/inference methodology for evaluating security risk with multiple uncertain information in SRA process. After reviewing the existing approaches and the factors that influence the security risk calculation and evaluation, the remainder of this chapter is organized as follows: In Section 5.2, theoretical background information for the proposed approach is represented. The proposed model and its process flow are introduced in Section 5.3. The illustrative application of the proposed approach is performed over an airport case study in Section 5.4. This section also examines the utility of findings and discusses the analysis results. Conclusions and further issues are addressed respectively in the final section.

5.2 Theoretical Background for Security Risk Evaluation

In this section, theoretical background information on rule-based expert systems and Linguistic Aggregation operators are presented, respectively**.**

5.2.1 Rule-based expert systems

In the literature, rule-based expert systems are used as a way to store and manipulate knowledge to interpret information in a useful way by emulating the decision-making ability of a human expert (Ross, 1995). They are often used in artificial intelligence applications and research as the domain-specific expert systems that use rules to make deductions or choices (Jackson, 1998). Typical rule based systems have two main components: a rule-base and an inference engine. A rule base is a list of rules, which is a specific type of knowledge base. Knowledge is stored as if-then rules in the rule-base. An inference engine infers information or takes action based on the interaction of input and the rule base.

There are two common inference techniques in the literature: Mamdani method and Sugeno method (Ross, 1995; Jang et al., 1997). The most commonly used inference technique is the so-called Mamdani method. In 1975, Professor Ebrahim Mamdani

built one of the first fuzzy systems to control a steam engine and boiler combination. He applied a set of fuzzy rules supplied by experienced human operators (Mamdani and Assilian, 1976). The format of the Mamdani-style fuzzy rule is as follows:

IF x is A $\oplus$ y is B THEN z is C **(5.1)**

where x, y and z are linguistic variables; A, B and C are fuzzy sets on universe of discourses X,Y and Z, respectively. An antecedent of a rule is linked by $\oplus$ connective that is a logical connective to represent relationship.

Mamdani method is widely accepted for capturing expert knowledge. It allows describing the expertise in more intuitive, more human-like manner. However, Mamdani-type fuzzy inference entails a substantial computational burden (Ross, 1995; Jang et al., 1997). Mamdani-style inference requires finding the centroid of a two-dimensional shape by integrating across a continuously varying function. In general, this process is not computationally efficient.

Michio Sugeno suggested using a singleton, as the membership function of the rule consequent (Jang et al., 1997). Sugeno-style fuzzy inference is very similar to the Mamdani method. Sugeno changed only a rule consequent. Instead of a fuzzy set, he used a mathematical function of the input variable. A singleton is a set with a membership function that is unity at a single particular point on the universe of discourse and zero everywhere else. The most commonly used zero-order Sugeno fuzzy model applies fuzzy rules in the following form:

IF x is A $\oplus$ y is B THEN z is k **(5.2)**

where x, y and z are linguistic variables; A and B are fuzzy sets on universe of discourses X and Y, respectively; and k is a constant. In this case, the output of each fuzzy rule is constant. All consequent membership functions are represented by singletons. Sugeno method is computationally effective and works well with optimisation and adaptive techniques, which makes it very attractive in control problems, particularly for dynamic nonlinear systems.

In this study, Sugeno method is adopted for REM. Sugeno method is used for the purpose of aggregating security risk factors in a nonlinear manner based on a rule base. Details of the application of Sugeno method are described in the next sections.

5.2.2 Linguistic aggregation

In the literature, many linguistic aggregation operators exist (Merigo and Casanovas 2010; Xu, 2004). In this section, main properties of uncertain linguistic aggregation operators and uncertain linguistic weighted average (ULWA) operator to be used throughout this chapter are described briefly.

Let $S = \{s_i \mid i = 1, ..., t\}$ is a finite and totally ordered discrete term set, where s_i represents a possible value for a linguistic variable (Xu, 2004). For example, a set of five terms S could be:

S = {s_1 = very low, s_2 = low, s_3 = medium, s_4 = high, s_5 = very high}

Main characteristics of set S are:

- ordered set : $s_i \geq s_j$ if $i \geq j$ **(5.3)**
- Max operator : $\max(s_i, s_j) = s_i$ if $s_i \geq s_j$ **(5.4)**
- Min operator : $\min(s_i, s_j) = s_i$ if $s_i \leq s_j$ **(5.5)**
- Negation operator : $neg(s_i) = s_j$ such that $j = t - i$ **(5.6)**

The discrete term set S is extended to a continuous term set $\overline{S} = \{s_\alpha \mid s_1 \leq s_\alpha \leq s_t, \alpha \in [1, t]\}$, whose elements also meet characteristics above. If $s_\alpha \in S$, s_α is called the original term, otherwise, s_α is called the virtual term. Let $\overline{s} = [s_\alpha, s_\beta]$, where $s_\alpha, s_\beta \in \overline{S}$, and s_α and s_β are the lower and the upper limits respectively. Therefore, $\overline{s}$ is called the uncertain linguistic variable.

Consider any two uncertain linguistic variables $\overline{s}_1 = [s_{\alpha_1}, s_{\beta_1}]$ and $\overline{s}_2 = [s_{\alpha_2}, s_{\beta_2}]$ then their operational laws are defined as follows:

- Commutativity : $\overline{s}_1 \oplus \overline{s}_2 = \overline{s}_2 \oplus \overline{s}_1$ **(5.7)**
- Addition : $\overline{s}_1 \oplus \overline{s}_2 = [s_{\alpha_1}, s_{\beta_1}] \oplus [s_{\alpha_2}, s_{\beta_2}]$ **(5.8)**

  $= [s_{\alpha_1} \oplus s_{\alpha_2}, s_{\beta_1} \oplus s_{\beta_2}] = [s_{\alpha_1 + \alpha_2}, s_{\beta_1 + \beta_2}]$
- Scalar product : $\overline{s}_1 = \lambda[s_{\alpha_1}, s_{\beta_1}] = [\lambda s_{\alpha_1}, \lambda s_{\beta_1}] = [s_{\lambda\alpha_1}, s_{\lambda\beta_1}]$, $\lambda \in [0,1]$ **(5.9)**
- $\lambda(\overline{s}_1 \oplus \overline{s}_2) = \lambda\overline{s}_1 \oplus \lambda\overline{s}_2$, $\lambda \in [0,1]$ **(5.10)**
- $(\lambda_1 \oplus \lambda_2)\overline{s}_1 = \lambda_1\overline{s}_1 \oplus \lambda_2\overline{s}_1$, $\lambda \in [0,1]$ **(5.11)**

An ULWA operator of dimension n is a mapping ULWA: $\overline{S}^n \to \overline{S}$ that has associated n vector w = $(w_1,w_2,\ldots,w_n)^T$ such that $w_i \in [0,1]$, i = 1,2,…,n, and $\sum_{i=1}^{n} w_i = 1$.

$$\mathrm{ULWA}(\overline{s}_1, \overline{s}_2, ..., \overline{s}_n) = \sum_{i=1}^{n} w_i \overline{s}_i \qquad \textbf{(5.12)}$$

For example, assume $\overline{s}_1 = [s_1, s_3]$, $\overline{s}_2 = [s_2, s_3]$, $\overline{s}_3 = [s_1, s_2]$, and w = $(0.3, 0.5, 0.2)^T$ then ULWA is calculated as follows (Eq. 5.1):

$$\begin{aligned}\mathrm{ULWA}(\overline{s}_1, \overline{s}_2, \overline{s}_3) &= 0.3*[s_1, s_3] \oplus 0.5*[s_2, s_3] \oplus 0.2*[s_1, s_2] \\ &= [s_{0.3}, s_{0.9}] \oplus [s_1, s_{1.5}] \oplus [s_{0.2}, s_{0.4}] \\ &= [s_{1.5}, s_{2.8}]\end{aligned}$$

In this study different from previous studies, the consequent of a rule is defines as an uncertain linguistic variable and the ULWA operator is used to aggregate activated rules in Sugeno method. The reasons for using the uncertain linguistic variable and ULWA operator and how ULWA operator is applied for the activated rule aggregation in Sugeno inference method is described in the following sections.

5.3 Rule-based Expert System for Security Risk Evaluation Model

In this study, new rule based expert system is proposed for aggregating threat likelihood, vulnerability and consequence information for evaluating security risk. Proposed method captures nonlinear causal relationships between security risk factors (threat likelihood, vulnerability and consequence) which have different uncertainty modes.

As security risk factors must be aggregated in a nonlinear manner, the relationship between security risk factors and a specific security risk level can be regarded as a rule. Once given an input, rule based system can be used to inference and generate an output. Given security factors and its strength, a rule makes one infers the possible presence of a specific security risk level or not in a nonlinear manner.

In a rule-based system, a rule is used to describe causal relationships between antecedent attributes and their associated consequent. Rule-based expert systems are

constructed from human judgments and domain knowledge in the form of if-then rules. For example, typical if-then rule for SRA is:

IF *Threat Likelihood is "Highly Likely"* **AND** *Vulnerability is "High"* **AND** *Consequence is "High"* **THEN** *Security Risk is "High-Very High"*

Therefore, SRA is a three input-one output problem. If–then rules are normally based on linguistic variables because they are more natural and expressive than numerical numbers. Linguistic rule base can capture sophisticated inferences with a reasonable effort. This allows using a linguistic approach to process quantitative information. Using linguistic variables instead of precise numbers are more appropriate for analysis using these three parameters as they are always associated with great uncertainty. Therefore, transforming quantitative data in the form of linguistic variables into a format that can be used along with qualitative data is required.

Both the Mamdani-style and Sugeno-style inference process is performed in four steps: fuzzification of the input variables, rule evaluation, aggregation of the rule outputs, and defuzzification. But these inference methods can not be directly applied to REM, because outputs from different models with different uncertainty modes could be implemented.

Knowledge representation, handling various types of uncertain input information is investigated first. Output information of models as an input information to proposed method are represented by the matching degree of referential values describing the attributes of antecedent of a rule using a two-dimensional variable. The output information of models is converted into a matching degree of referential values by using fuzzification and bet estimate. By this way, different formats of available data and various types of uncertainties such as ignorance and vagueness in inference process can be incorporated into REM process.

Because of the arbitrary numeric scales problem mentioned in Section 5.1, the consequent of a rule is neither fuzzy set like in Mamdani-style inference nor constant like in Mamdani-style inference. Different from previous studies, the consequent of a rule is uncertain linguistic variables in this study. This definition also allows consequents to be either individual grades or subsets of adjacent grades, intervals such as "High-Very High" interval grades.

Since the consequent of rules are uncertain linguistic variables, rule aggregation of the proposed method is also different from typical inference methods. In Sugeno method, weighted average (WA) is used to aggregate activated rules. However, the WA operator can only be used in situations where the input arguments are exact numerical values. But in this study, consequent of a rule in the rule base is determined as an uncertain linguistic variable. Therefore, the ULWA operator is used for rule aggregation where the consequent of rules are uncertain linguistic variables. A rule base constructed by the rules given in the form above represents functional mappings between antecedents and consequents. It provides a more informative and realistic scheme for various uncertain knowledge representation. When a rule base is established, the knowledge contained in the rule base can be used to perform security risk inference of a critical facility for given inputs. The inference procedure is investigated in the following subsections.

The proposed approach consists of the following steps shown in Figure 5.1.

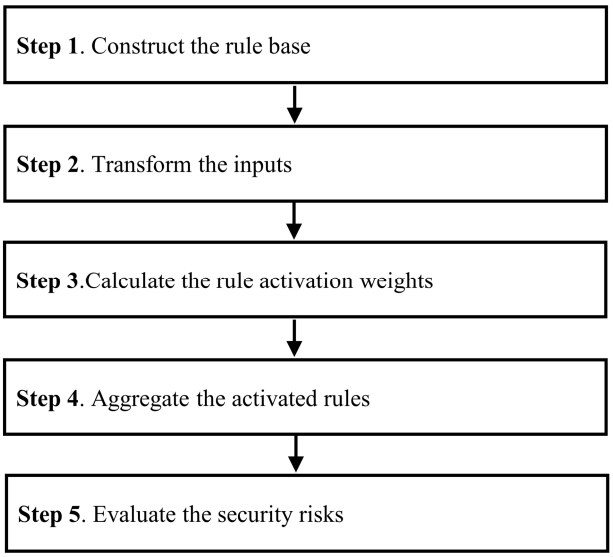


Figure 5.1 : Steps of proposed approach.

Step 1: Construct the rule base

The starting point of constructing a rule-based system is to collect if–then rules from human experts based on domain knowledge. Then a knowledge base and an inference engine are designed to infer useful conclusions from the rules and inputs provided by output of SRA models. Suppose a rule base is given by $R = \{R_1, \ldots, R_k, \ldots, R_L\}$. L is the total number of rules in the rule base. Formally, the kth rule, R_k, in a rule base can be written as

$$R_k : IF\ H_1^k \oplus ... \oplus H_i^k \oplus ... \oplus H_M^k\ THEN\ \bar{H}_{pq}^k \quad \textbf{(5.13)}$$

where H_i^k (i=1,..,M) is a referential value of the ith antecedent attribute in the kth rule, and M is the number of the antecedent attributes used in the kth rule. $H^k = \{H_1^k, ..., H_i^k, ..., H_M^k\}$ is the packet antecedent in the kth rule. $\bar{H}_{pq}^k$ is an uncertain linguistic variable referential value of the consequent where $\bar{H}_{pq}^k = [H_p, H_q]$. An antecedent of a rule is linked by $\oplus$ connective that is a logical connective to represent relationship. Since, each rule has multiple antecedents, both disjunctive opertor and conjunctive operator are used for the rule antecedent evaluation in this study. To evaluate the disjunction of the rule antecedents, the OR ($\vee$) operation is applied as:

$$R_k^{\vee} : IF\ H_1^k \vee ... \vee H_i^k \vee ... \vee H_M^k\ THEN\ \bar{H}_{pq}^k \quad \textbf{(5.14)}$$

Similarly, in order to evaluate the conjunction of the rule antecedents, the AND ($\wedge$) operation is applied as:

$$R_k^{\wedge} : IF\ H_1^k \wedge ... \wedge H_i^k \wedge ... \wedge H_M^k\ THEN\ \bar{H}_{pq}^k \quad \textbf{(5.15)}$$

A referential value describing the attributes of antecedent H_i^k and consequent $\bar{H}_{pq}^k$ is a H_{pq} (p,q=1,...,N) evaluation grade where H_{pp} are individual evaluation grade, and H_{pq} for p=1 to N and q=p+1 to N-1 is the interval evaluation grade between H_{pp} and H_{qq} in this study. H_{pp} (p=1,...,N) are mutually exclusive. Therefore, a set of evaluation grades for each referential value is denoted by

$$H = \{H_{pq}, \mathrm{p} = \mathrm{q}, \mathrm{p} = 1, ..., \mathrm{N}\} \quad \textbf{(5.16)}$$

H_{11} and H_{NN} are set to be the worst and the best grades, respectively, and H_{p+1p+1} is to be preferred to H_{pp} among evaluation grades. Therefore, a basic rule base is composed of if-then rules as in Equation 5.14 and Equation 5.15.

Step 2: Transform the input

Before starting an inference process, the relationship between an input and each referential value in the antecedents of a rule needs to be determined so that an activation weight for each rule can be generated. The basic idea is to examine all the referential values of each attribute in order to determine a similarity/matching degree to which an input belongs to a referential value.

The matching degree of referential values describing the attributes of antecedent of a rule is provided by the outputs of SRA models. Transformation of input variables from different models with different uncertainty modes is implemented in this step. Inputs are transformed into matching degree of referential values. After transformations, a general input form corresponding to all antecedent attributes is given as

$$H^* = \{(H^*_{i,j}, \beta^*_{ij})\}, i = 1,...,M,\ j = 1,...,T_i\} \quad \textbf{(5.17)}$$

where β^*_{ij} expresses the matching degree assigned to the input $H^*_{i,j}$, the jth referential value of ith attribute. T_i is the total number of number of the referential values used for describing the ith antecedent attribute and M is the total number of antecedent attributes involved in all the rules in a rule base.

For example, an input in REM transformed into the any rule is given by Threat Likelihood is {(highly likely, 0.8)} and Vulnerability is {(high,0.3),(medium,0.7)} and consequence is {(high,0.3),(medium,0.7)}.

Step 3: Calculate the rule activation weights

At this step the rule activation weights are calculated. Once the matching degree between an input and the referential values of all antecedents in a rule are determined, they are processed to generate an activation weight for the rule which is used to measure the degree to which the packet antecedent of the rule k, H^k, is activated by the input.

Since, each rule has multiple antecedents, both disjunctive operator and conjunctive operator are used to obtain a single number that represents the result of the rule antecedent evaluation for the purpose of sensitivity analysis. To evaluate the disjunction of the rule antecedents, the OR ($\vee$) operation is applied (Eq. 5.14). Similarly, in order to evaluate the conjunction of the rule antecedents, the AND ($\wedge$) operation is applied (Eq. 5.15).

Given the input for the packet antecedent H^k in the kth rule, denoted by H^* and the corresponding activation weight (w_k) to which the input matches the packet antecedent H^k in the kth rule can be calculated using the following formulas:

$$w_k^{\vee} = \max(\beta^*_{ij}), i = 1,...,M, H_{i,j} \in H^k\ \forall i, j \quad \textbf{(5.18)}$$

$$w_k^{\wedge} = \min(\beta_{ij}^*), i = 1,...,M, H_{i,j} \in H^k \ \forall i, j \quad \textbf{(5.19)}$$

where β_{ij}^* expresses the matching degree assigned to the input $H_{i,j}^*$, the jth referential value of ith attribute and M is the total number of antecedent attributes involved in all the rules in a rule base. Note that $0 \leq w_k \leq 1$ and $w_k=0$ if the kth rule is not activated. w_k is the activation weight of rule k which measures the degree to which the kth rule is weighted and activated. Input activates different rules depending on activation weights of each rule. The activation weights w_k for all the rules R_k (k = 1,…, K) are generated using Equations 5.18-5.19.

Step 4: Aggregate the activated rules

At this step, the inference procedure is implemented in order to combine all rules for generating the final matching degree for activated rules of a scenario. Since consequent is uncertain linguistic variable, ULWA operator is employed to combine the activated rules in this study.

Let $R' = \{R_1,..., R_k, ...R_{L'}\}$ set of L' rules which are activated by the actual input H^* and the inference of a rule-based system is implemented using the linguistic aggregation operator as :

$$\bar{H}_{\alpha\beta}^{\vee} = ULWA_{\vee}(H^*) = \sum_{k=1}^{L'} w_k^{\vee} \bar{H}_{pq}^k \quad \textbf{(5.20)}$$

$$\bar{H}_{\alpha\beta}^{\wedge} = ULWA_{\wedge}(H^*) = \sum_{k=1}^{L'} w_k^{\wedge} \bar{H}_{pq}^k \quad \textbf{(5.21)}$$

where $\bar{H}_{\alpha\beta}^{\vee/\wedge}$ is the final matching degree for activated rules of a scenario in the form of an uncertain linguistic variable where $\bar{H}_{\alpha\beta}^{\vee/\wedge} = [H_\alpha, H_\beta]$, w_k is the activation weight of the kth rule, and $\bar{H}_{pq}^k$ is an uncertain linguistic variable referential value of the consequent where $\bar{H}_{pq}^k = [H_p, H_q]$. The final result generated by aggregating the L' rules, which are activated by the actual input vector H^* of a scenario is represented in the form of an uncertain linguistic variable, $\bar{H}_{\alpha\beta}^{\vee/\wedge}$, that is produced by ULWA operator.

Step 5: Evaluate the security risk

In order to evaluate the identified scenarios, the security risk of identified scenarios is needed to be ranked and compared based on their uncertain linguistic variables which are also intervals. Therefore, ranking of identified scenarios based on their intervals is required. For this purpose, preference function proposed by Wang is adopted (Wang et al., 2005; Wang et al., 2006). The properties of Wang's method are discussed in Chapter 2 in detail.

Let $H_{\alpha_A\beta_A}$ and $H_{\alpha_B\beta_B}$ be the uncertain linguistic variables of A and B respectively. Then the degree of preference of A over B, denoted by P(A > B) ∈ [0, 1], is defined as follows:

$$P(A > B) = \frac{\max[0, \beta_A - \alpha_B] - \max[0, \alpha_A - \beta_B]}{[\beta_A - \alpha_A] + [\beta_B - \alpha_B]} \quad \textbf{(5.22)}$$

Therefore, based on the properties of preference function, A is superior to B if $P(A>B)$ > 0.5, A is indifferent to B if $P(A>B)$ = 0.5, and A is inferior to B if $P(A>B)$ < 0.5. The preference function between scenarios has transitivity, i.e., if scenario A is superior to B, and scenario B is superior to C, then scenario A is superior to C. By applying Eq. 5.22, preference relations among all scenarios can be determined for any evaluation grade, H_{pp}.

5.4 An Illustrative Example for Security Risk Evaluation

In this section, the proposed rule based expert system approach as described in Section 5.3 is applied to a hypothetical Airport X to evaluate security risk of identified threat scenarios. Note that for security reasons, all the data used throughout this example are purely generic and notional. Even though this case study is very simple, the resulting qualitative relationships and insights drawn from this example validate the proposed approach. A step-by-step algorithm for this example is as follows:

Step 1: Construct the rule base

Typical If-then rules for REM are defined based on Equation 5.13-15 as follows:

$$R_k^{\vee} : IF\ H_1^k \vee H_2^k \vee H_3^k\ THEN\ \bar{H}_{pq}^k \quad \textbf{(5.23)}$$

$$R_k^{\wedge} : IF\ H_1^k \wedge H_2^k \wedge H_3^k\ THEN\ \bar{H}_{pq}^k \quad \textbf{(5.24)}$$

where H_1^k is the referential value of antecedent attribute threat likelihood (T), H_2^k is the referential value of antecedent attribute vulnerability (V) and H_3^k is the referential value of antecedent attribute consequence (C), respectively. The number of antecedent attributes used in any rule for REM, M, is 3. $\bar{H}_{pq}^k$ is the uncertain linguistic variable referential value of consequent attribute security risk (SR).

The granularity of linguistic term sets used for describing each fundamental factor is decided according to the situation of the case of interest. In the literature, the granularity from three to nine labels is commonly used to represent any factor. Therefore, the referential value set of defined attributes are determined as follows:

- The referential value set for threat likelihood is given by

  T = {“Likely” (H_1), “Very Likely” (H_2), “Highly Likely” (H_3), “Very Highly Likely” (H_4), ”Extremely Likely” (H_5)}.

- The referential value set for vulnerability is given by

  V = {“Low” (H_1), “Medium” (H_2), “High” (H_3)}.

- The referential value set for consequence is given by

  C = {“Very Low” (H_1), “Low” (H_2), “Medium” (H_3), “High” (H_4), “Very High” (H_5)}.

- The referential value set for security risk is given by

  SR = {“Very Low” (H_{11}), “Low” (H_{22}), “Medium” (H_{33}), “High” (H_{44}), “Very High” (H_{55})}

$$H = \begin{Bmatrix} H_{11} & H_{12} & H_{13} & H_{14} & H_{15} \\ & H_{22} & H_{23} & H_{24} & H_{25} \\ & & H_{33} & H_{34} & H_{35} \\ & & & H_{44} & H_{45} \\ & & & & H_{55} \end{Bmatrix} = \begin{Bmatrix} VL & VL-L & VL-M & VL-H & VL-VH \\ & L & L-M & L-H & L-VH \\ & & M & M-H & M-VH \\ & & & H & H-VH \\ & & & & VH \end{Bmatrix}$$

Organizations differ in the amount of risk they are willing to accept. Preference for risk and interpretation of risk differ. Such if-then rules are collected from security

experts based on domain knowledge that constitute a rule base with both individual and interval based grades and L=5*3*5=75 rules are defined:

$R = \{R_1, \ldots, R_{75}\}$ **(5.25)**

Sample rule base for security risk evaluation of Airport X is given in Table 5.2. When sample rule base is examined, rules R_1-R_5 have the minimum security risk and rules R_{71}- R_{75} have the maximum security risk. High Likelihood – Low Consequence rules are R_1-R_5 and Low Likelihood – High Consequence rules are R_1-R_5. Based on the domain knowledge, the rules are interpreted differently in a nonlinear manner rather than linear.

Step 2: Transform the input

Since the matching degree of referential values describing the attributes of antecedent of a rule is needed for the input of REM, the outputs of SRA models are transformed into the required form of Equation 5.17 in this step. The input is given as linguistic terms with the matching degrees based on the three models described in the previous chapters. The fuzzification is applied to VAM and CAM, and bet estimate is applied to TAM in this study. The details of the transformation for the models are described in the following sub sections.

Step 2.1 : Transform TAM output

In TAM, DST is used for uncertainty modelling and the output data for threat likelihood are represented by DST variables due to epistemic uncertainty. Bet estimate gives a point estimate in a belief structure similar to defuzzification in the fuzzy set theory as follows (Smets, 2000):

$$bet(A) = \sum_{A \subseteq B} \frac{m(B)}{|B|} \quad \textbf{(5.26)}$$

where $|B|$ is the cardinality (number of elements) in the set B. For example, as a belief structure of threat scenario 1 is $\{(H_{33}, 0.0269), (H_{34}, 0.0022), (H_{44}, 0.0134), (H_{55}, 0.0131), (\Theta, 0.9444)\}$, bet estimate of this scenario is calculated as:

$$bet(H_3) = \frac{m(H_3)}{1} + \frac{m(H_{34})}{2} + \frac{m(\Theta)}{5} = 0.0269 + 0.0011 + 0.1889 = 0.2169$$

Bet estimates of likelihood belief structures of identified threat scenarios are calculated and results are presented in Table 5.3.

Table 5.2 : Sample rule base.

IF Antecedent (H^k) **THEN** Consequent (H^k_{pq})									
Antecedent				Consequent		Antecedent				Consequent
No	***TL***	***V***	***C***	***SR***		***No***	***TL***	***V***	***C***	***SR***
1	H_1	H_1	H_1	H_{11}		39	H_5	H_2	H_1	H_{33}
2	H_1	H_1	H_2	H_{11}		40	H_2	H_2	H_5	H_{33}
3	H_2	H_1	H_1	H_{11}		41	H_4	H_2	H_2	H_{33}
4	H_2	H_1	H_2	H_{11}		42	H_3	H_2	H_4	H_{34}
5	H_1	H_1	H_3	H_{11}		43	H_5	H_2	H_2	H_{34}
6	H_1	H_1	H_4	H_{12}		44	H_3	H_2	H_5	H_{44}
7	H_3	H_1	H_1	H_{12}		45	H_4	H_2	H_3	H_{44}
8	H_2	H_1	H_3	H_{12}		46	H_4	H_2	H_4	H_{45}
9	H_1	H_1	H_5	H_{22}		47	H_5	H_2	H_3	H_{45}
10	H_4	H_1	H_1	H_{22}		48	H_4	H_2	H_5	H_{55}
11	H_2	H_1	H_4	H_{22}		49	H_5	H_2	H_4	H_{55}
12	H_3	H_1	H_2	H_{22}		50	H_5	H_2	H_5	H_{55}
13	H_3	H_1	H_3	H_{23}		51	H_1	H_3	H_1	H_{11}
14	H_5	H_1	H_1	H_{23}		52	H_1	H_3	H_2	H_{12}
15	H_2	H_1	H_5	H_{23}		53	H_2	H_3	H_1	H_{12}
16	H_4	H_1	H_2	H_{23}		54	H_2	H_3	H_2	H_{22}
17	H_3	H_1	H_4	H_{33}		55	H_1	H_3	H_3	H_{22}
18	H_5	H_1	H_2	H_{33}		56	H_1	H_3	H_4	H_{23}
19	H_3	H_1	H_5	H_{34}		57	H_3	H_3	H_1	H_{23}
20	H_4	H_1	H_3	H_{34}		58	H_2	H_3	H_3	H_{23}
21	H_4	H_1	H_4	H_{44}		59	H_1	H_3	H_5	H_{33}
22	H_5	H_1	H_3	H_{44}		60	H_4	H_3	H_1	H_{33}
23	H_4	H_1	H_5	H_{45}		61	H_2	H_3	H_4	H_{33}
24	H_5	H_1	H_4	H_{45}		62	H_3	H_3	H_2	H_{33}
25	H_5	H_1	H_5	H_{55}		63	H_3	H_3	H_3	H_{34}
26	H_1	H_2	H_1	H_{11}		64	H_5	H_3	H_1	H_{34}
27	H_1	H_2	H_2	H_{11}		65	H_2	H_3	H_5	H_{34}
28	H_2	H_2	H_1	H_{11}		66	H_4	H_3	H_2	H_{34}
29	H_2	H_2	H_2	H_{12}		67	H_3	H_3	H_4	H_{44}
30	H_1	H_2	H_3	H_{12}		68	H_5	H_3	H_2	H_{44}
31	H_1	H_2	H_4	H_{22}		69	H_3	H_3	H_5	H_{45}
32	H_3	H_2	H_1	H_{22}		70	H_4	H_3	H_3	H_{45}
33	H_2	H_2	H_3	H_{22}		71	H_4	H_3	H_4	H_{55}
34	H_1	H_2	H_5	H_{23}		72	H_5	H_3	H_3	H_{55}
35	H_4	H_2	H_1	H_{23}		73	H_4	H_3	H_5	H_{55}
36	H_2	H_2	H_4	H_{23}		74	H_5	H_3	H_4	H_{55}
37	H_3	H_2	H_2	H_{23}		75	H_5	H_3	H_5	H_{55}
38	H_3	H_2	H_3	H_{33}						

Table 5.3 :TAM output.

Threat scenario		Threat Likelihood					
		H_1	H_2	H_3	H_4	H_5	Rank
1	$(a_3^1, a_1^2, a_1^3, a_1^4)$	-	-	0.2169	0.2034	0.2020	3
2	$(a_3^1, a_1^2, a_2^3, a_1^4)$	-	-	0.2119	-	-	7
3	$(a_3^1, a_1^2, a_1^3, a_2^4)$	-	-	0.2336	0.2067	-	6
4	$(a_3^1, a_1^2, a_2^3, a_2^4)$	0.2023	0.2083	0.2003	-	-	11
5	$(a_4^1, a_2^2, a_2^3, a_1^4)$	-	-	0.2101	-	-	8
6	$(a_4^1, a_2^2, a_2^3, a_2^4)$	-	-	0.2077	-	-	9
7	$(a_5^1, a_1^2, a_1^3, a_1^4)$	-	-	0.2025	0.2025	0.2025	1
8	$(a_5^1, a_1^2, a_2^3, a_1^4)$	0.2003	0.2003	0.2076	-	-	10
9	$(a_5^1, a_1^2, a_1^3, a_2^4)$	-	-	0.2064	0.1994	0.1994	2
10	$(a_5^1, a_1^2, a_2^3, a_2^4)$	0.2335	0.2104	0.1901	-	-	12
11	$(a_{11}^1, a_1^2, a_1^3, a_1^4)$	-	0.1906	0.2435	0.1894	0.1894	5
12	$(a_{11}^1, a_1^2, a_1^3, a_2^4)$	-	-	0.2323	0.1927	0.1927	4

Step 2.2 : Transform VAM output

In VAM, the fuzzy set theory is used for uncertainty modelling and the output data for vulnerability are represented by vulnerability scores. Fuzzification is the process of making a crisp quantity fuzzy by taking the crisp input and determining the degree to which this input belongs to each of the appropriate fuzzy sets. Therefore, vulnerability can be quantified by the degree of membership of a numerical value to a fuzzy set. The output of VAM is described using linguistic variables given in Table 5.4 and each linguistic variable is indicated by a TFN within the interval of [0, 1]. The linguistic variables in Table 5.4 and their membership functions are shown in Figure 5.2.

By using the linguistic variables in Table 5.4 and their membership functions shown in Figure 5.1, vulnerability scores are fuzzified and results are presented for the identified threat scenarios in Table 5.5.

Table 5.4 : Linguistic variables for the vulnerability of targets.

Linguistic variable	**Triangular fuzzy number**
Low (L)	(0, 0, 0.5)
Medium (M)	(0, 0.5,1)
High (H)	(0.5, 1, 1)

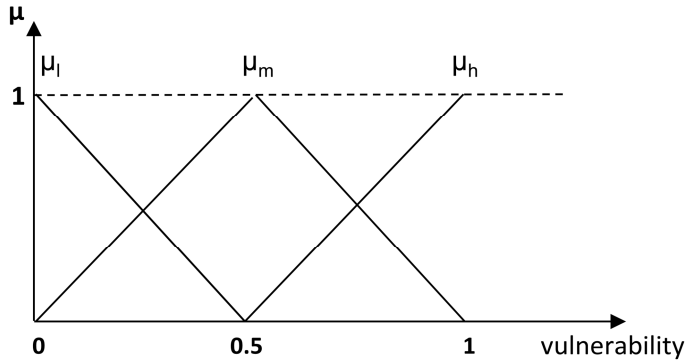


Figure 5.2 : Membership functions of linguistic variables for vulnerability.

Table 5.5 :VAM output.

Target	Vulnerability	Rank	Normalized Vulnerability	Vulnerability		
				H_1	H_2	H_3
a_1^1	1.202	4	0.581	-	0.838	0.162
a_2^1	1.183	5	0.572	-	0.856	0.144
a_3^1	0.919	8	0.444	0.112	0.888	-
a_4^1	0.710	14	0.343	0.314	0.686	-
a_5^1	0.763	12	0.369	0.262	0.738	-
a_6^1	0.889	9	0.430	0.140	0.860	-
a_7^1	1.033	7	0.499	0.002	0.998	
a_8^1	1.090	6	0.527	-	0.946	0.054
a_9^1	0.742	13	0.359	0.282	0.718	-
a_{10}^1	0.814	10	0.393	0.214	0.786	-
a_{11}^1	0.648	15	0.313	0.374	0.626	-
a_{12}^1	0.606	16	0.293	0.414	0.586	-
a_{13}^1	0.803	11	0.388	0.224	0.776	-
a_{14}^1	0.583	17	0.282	0.436	0.564	-
a_{15}^1	0.425	19	0.205	0.590	0.410	-
a_{16}^1	0.541	18	0.262	0.476	0.524	-
a_{17}^1	0.424	20	0.204	0.592	0.408	-
a_{18}^1	1.272	3	0.615	-	0.770	0.230
a_{19}^1	2.069	1	1.000	-	-	1.000
a_{20}^1	1.291	2	0.624	-	0.752	0.248

Step 2.3: Transform CAM output

In CAM, probability theory is used for uncertainty modelling and the output data for consequence are represented by random variables due to stochastic uncertainty. By using the expected values of consequence, consequence can be quantified by the degree of membership of a numerical value to a fuzzy set like the fuzzification of vulnerability score. The output of CAM is described using linguistic variables given in Table 5.6 and each linguistic variable is indicated by a TFN within the interval of [0, 1]. The linguistic variables in Table 5.6 and their membership functions are shown in Figure 5.3.

Table 5.6 : Linguistic variables for the consequence of threat scenarios.

Linguistic variable	**Triangular fuzzy number**
Very low (VL)	(0, 0, 0.3)
Low (L)	(0.1, 0.3, 0.5)
Medium (M)	(0.3, 0.5, 0.7)
High (H)	(0.5, 0.7, 1)
Very High (VH)	(0.7, 1, 1)

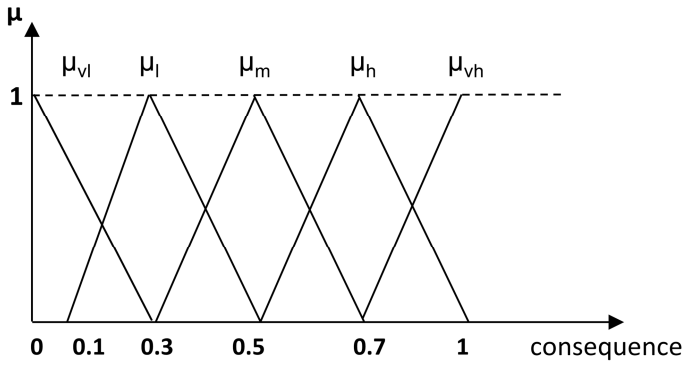


Figure 5.3 : Membership functions of linguistic variables for consequence.

By using the linguistic variables in Table 5.6 and their membership functions shown in Figure 5.3, expected values of consequence are fuzzified and results are presented for the identified threat scenarios in Table 5.7.

The fuzzification is applied to VAM and CAM, and bet estimate is applied to TAM for transforming the input in the required form of Equation 5.17 in this study. All the transformed inputs for the identified threat scenarios are shown in Table 5.8.

Table 5.7 :CAM output.

Threat Scenario	Consequence	Rank	Normalized Consequence	Consequence				
				H_1	H_2	H_3	H_4	H_5
1 $(a_3^1, a_1^2, a_1^3, a_1^4)$	2,557,497	10	0.1305	0.5650	0.1525	-	-	-
2 $(a_3^1, a_1^2, a_2^3, a_1^4)$	5,776,055	3	0.2948	0.0174	0.9740	-	-	-
3 $(a_3^1, a_1^2, a_1^3, a_2^4)$	3,360,789	7	0.1715	0.4284	0.3575	-	-	-
4 $(a_3^1, a_1^2, a_2^3, a_2^4)$	8,477,618	2	0.4326	-	0.3370	0.6630	-	-
5 $(a_4^1, a_2^2, a_2^3, a_1^4)$	4,871,782	5	0.2486	0.1714	0.7430	-	-	-
6 $(a_4^1, a_2^2, a_2^3, a_2^4)$	13,913,540	1	0.7100	-	-	-	0.9667	0.0334
7 $(a_5^1, a_1^2, a_1^3, a_1^4)$	1,879,900	12	0.0959	0.6804	-	-	-	-
8 $(a_5^1, a_1^2, a_2^3, a_1^4)$	3,755,768	6	0.1917	0.3610	0.4585	-	-	-
9 $(a_5^1, a_1^2, a_1^3, a_2^4)$	2,632,710	9	0.1344	0.5520	0.1720	-	-	-
10 $(a_5^1, a_1^2, a_2^3, a_2^4)$	5,526,108	4	0.2820	0.0600	0.9100	-	-	-
11 $(a_{11}^1, a_1^2, a_1^3, a_1^4)$	2,105,731	11	0.1075	0.6417	0.0375	-	-	-
12 $(a_{11}^1, a_1^2, a_1^3, a_2^4)$	2,899,042	8	0.1479	0.5070	0.2395	-	-	-

Table 5.8 : Transformed inputs.

N	$H^* = \{(H_{i,j}^*, \beta_{ij}^*)\}$		
	Threat Likelihood, i=1	Vulnerability, i=2	Consequence, i=3
1	$\{(H_{1,3},0.2169),(H_{1,4},0.2034),(H_{1,5},0.2020)\}$	$\{(H_{2,1},0.1120),(H_{2,2},0.8880)\}$	$\{(H_{3,1},0.5650),(H_{3,2},0.1525)\}$
2	$\{(H_{1,3},0.2119)\}$	$\{(H_{2,1},0.1120),(H_{2,2},0.8880)\}$	$\{(H_{3,1},0.0174),(H_{3,2},0.9740)\}$
3	$\{(H_{1,3},0.2336),(H_{1,4},0.2067)\}$	$\{(H_{2,1},0.1120),(H_{2,2},0.8880)\}$	$\{(H_{3,1},0.4284),(H_{3,2},0.3575)\}$
4	$\{(H_{1,1},0.2023),(H_{1,2},0.2083),(H_{1,3},0.2003)\}$	$\{(H_{2,1},0.1120),(H_{2,2},0.8880)\}$	$\{(H_{3,2},0.3370),(H_{3,3},0.6630)\}$
5	$\{(H_{1,3},0.2101)\}$	$\{(H_{2,1},0.3140),(H_{2,2},0.6860)\}$	$\{(H_{3,1},0.1714),(H_{3,2},0.7430)\}$
6	$\{(H_{1,3},0.2077)\}$	$\{(H_{2,1},0.3140),(H_{2,2},0.6860)\}$	$\{(H_{3,4},0.9667),(H_{3,5},0.0334)\}$
7	$\{(H_{1,3},0.2025),(H_{1,4},0.2025),(H_{1,5},0.2025)\}$	$\{(H_{2,1},0.2620),(H_{2,2},0.7380)\}$	$\{(H_{3,1},0.6804)\}$
8	$\{(H_{1,1},0.2003),(H_{1,2},0.2003),(H_{1,3},0.2076)\}$	$\{(H_{2,1},0.2620),(H_{2,2},0.7380)\}$	$\{(H_{3,1},0.3610),(H_{3,2},0.4585)\}$
9	$\{(H_{1,3},0.2064),(H_{1,4},0.1994),(H_{1,5},0.1994)\}$	$\{(H_{2,1},0.2620),(H_{2,2},0.7380)\}$	$\{(H_{3,1},0.5520),(H_{3,2},0.1720)\}$
10	$\{(H_{1,1},0.2335),(H_{1,2},0.2104),(H_{1,3},0.1901)\}$	$\{(H_{2,1},0.2620),(H_{2,2},0.7380)\}$	$\{(H_{3,1},0.0600),(H_{3,2},0.9100)\}$
11	$\{(H_{1,2},0.1906),(H_{1,3},0.2435)(H_{1,4},0.1894),(H_{1,5},0.1894)\}$	$\{(H_{2,1},0.3740),(H_{2,2},0.6260)\}$	$\{(H_{3,1},0.6417),(H_{3,2},0.0375)\}$
12	$\{(H_{1,3},0.2323),(H_{1,4},0.1927),(H_{1,5},0.1927)\}$	$\{(H_{2,1},0.3740),(H_{2,2},0.6260)\}$	$\{(H_{3,1},0.5070),(H_{3,2},0.2395)\}$

Step 3: Calculate the rule activation weights

The activation weights w_k for all the activated rules $R' = \{R_1, ..., R_k, ...R_{L'}\}$ are generated by using both disjunctive operator (OR (∨)) and conjunctive operator (AND (∧)) (Eqs. 5.18-19). For example, for threat scenario 1 following rules in Table 5.9 are activated for the transformed inputs in Table 5.8.

Table 5.9 : Activated rules for threat scenario 1.

Activated Rule	IF	Antecedent TL	∧/∨	Antecedent V	∧/∨	Antecedent C	THEN	Consequent SR	Activation weight $w_k^{\wedge}$	Activation weight $w_k^{\vee}$
7		H_3		H_1		H_1		H_{12}	0.1120	0.5650
12		H_3		H_1		H_2		H_{22}	0.1120	0.2169
32		H_3		H_2		H_1		H_{22}	0.2169	0.8880
37		H_3		H_2		H_2		H_{23}	0.1525	0.8880
10		H_4		H_1		H_1		H_{22}	0.1120	0.5650
16		H_4		H_1		H_2		H_{23}	0.1120	0.2034
35		H_4		H_2		H_1		H_{23}	0.2034	0.8880
41		H_4		H_2		H_2		H_{33}	0.1525	0.8880
14		H_5		H_1		H_1		H_{23}	0.1120	0.5650
18		H_5		H_1		H_2		H_{33}	0.1120	0.2020
39		H_5		H_2		H_1		H_{33}	0.2020	0.8880
43		H_5		H_2		H_2		H_{34}	0.1525	0.8880

The activation weight for rule 7 is calculated for the given input as follows:

$$w_7^{\wedge} = \min(0.2169, 0.1120, 0.5650) = 0.1120$$

$$w_7^{\vee} = \max(0.2169, 0.1120, 0.5650) = 0.5650$$

Activations weights for identified scenarios are calculated using both disjunctive operator and conjunctive operator and presented in Table 5.10 and Table 5.11.

Table 5.10 : $w_k^{\wedge}$ activation weights for threat scenarios.

No.	$S_t(.)$	Activation weights
1	$S_t(a_3^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{12},0.1120),(H_{22},0.1120),(H_{22},0.2169),(H_{23},0.1525),(H_{22},0.1120),$ $(H_{23},0.1120),(H_{23},0.2034),(H_{33},0.1525),(H_{23},0.1120),(H_{33},0.1120),$ $(H_{33},0.2020),(H_{34},0.1525)\}$
2	$S_t(a_3^1, a_1^2, a_2^3, a_1^4)$	$\{(H_{12},0.0174),(H_{22},0.1120),(H_{22},0.0174),(H_{23},0.2119)\}$
3	$S_t(a_3^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{12},0.1120),(H_{22},0.1120),(H_{22},0.2336),(H_{23},0.2336),(H_{22},0.1120),$ $(H_{23},0.1120),(H_{23},0.2067),(H_{33},0.2067)\}$
4	$S_t(a_3^1, a_1^2, a_2^3, a_2^4)$	$\{(H_{11},0.1120),(H_{11},0.1120),(H_{11},0.2023),(H_{12},0.2023),(H_{11},0.1120),$ $(H_{12},0.1120),(H_{12},0.2083),(H_{22},0.2083),(H_{22},0.1120),(H_{23},0.1120),$ $(H_{23},0.2003),(H_{33},0.2003)\}$
5	$S_t(a_4^1, a_2^2, a_2^3, a_1^4)$	$\{(H_{12},0.1714),(H_{22},0.2101),(H_{22},0.1714),(H_{23},0.2101)\}$
6	$S_t(a_4^1, a_2^2, a_2^3, a_2^4)$	$\{(H_{33},0.2077),(H_{34},0.0334),(H_{34},0.2077),(H_{44},0.0334)\}$
7	$S_t(a_5^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{12},0.2025),(H_{22},0.2025),(H_{22},0.2025),(H_{23},0.2025),(H_{23},0.2025),$ $(H_{33},0.2025)\}$
8	$S_t(a_5^1, a_1^2, a_2^3, a_1^4)$	$\{(H_{11},0.2003),(H_{11},0.2003),(H_{11},0.2003),(H_{11},0.2003),(H_{11},0.2003),$ $(H_{11},0.2003),(H_{11},0.2003),(H_{12},0.2003),(H_{12},0.2076),(H_{22},0.2076),$ $(H_{22},0.2076),(H_{23},0.2076)\}$
9	$S_t(a_5^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{12},0.2064),(H_{22},0.1720),(H_{22},0.2064),(H_{23},0.1720),(H_{22},0.1994),$ $(H_{23},0.1720),(H_{23},0.1994),(H_{33},0.1720),(H_{23},0.1994),(H_{33},0.1720),$ $(H_{33},0.1994),(H_{34},0.1720)\}$
10	$S_t(a_5^1, a_1^2, a_2^3, a_2^4)$	$\{(H_{11},0.0600),(H_{11},0.2335),(H_{11},0.0600),(H_{11},0.2335),(H_{11},0.0600),$ $(H_{11},0.2104),(H_{11},0.0600),(H_{12},0.2104),(H_{12},0.0600),(H_{22},0.1901),$ $(H_{22},0.0600),(H_{23},0.1901)\}$
11	$S_t(a_{11}^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{11},0.1906),(H_{11},0.0375),(H_{11},0.1906),(H_{12},0375),(H_{12},0.2435),$ $(H_{22},0.0375),(H_{22},0.2435),(H_{23},0.0375),(H_{22},0.1894),(H_{23},0.0375),$ $(H_{23},0.1894),(H_{33},0.0375),(H_{23},0.1894),(H_{33},0.0375),(H_{33},0.1894),$ $(H_{34},0.0375)\}$
12	$S_t(a_{11}^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{12},0.2323),(H_{22},0.2323),(H_{22},0.2323),(H_{23},0.2323),(H_{22},0.1927),$ $(H_{23},0.1927),(H_{23},0.1927),(H_{33},0.1927),(H_{23},0.1927),(H_{33},0.1927),$ $(H_{33},0.1927),(H_{34},0.1927)\}$

Table 5.11 : $w_k^{\vee}$ activation weights for threat scenarios.

No.	$S_t(.)$	Activation weights
1	$S_t(a_3^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{12},0.5650),(H_{22},0.2169),(H_{22},0.8880),(H_{23},0.8880),(H_{22},0.5650),(H_{23},0.2034),(H_{23},0.8880),(H_{33},0.8880),(H_{23},0.5650),(H_{33},0.2020),(H_{33},0.8880),(H_{34},0.8880)\}$
2	$S_t(a_3^1, a_1^2, a_2^3, a_1^4)$	$\{(H_{12},0.2119),(H_{22},0.9740),(H_{22},0.8880),(H_{23},0.9740)\}$
3	$S_t(a_3^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{12},0.4284),(H_{22},0.3575),(H_{22},0.8880),(H_{23},0.8880),(H_{22},0.4284),(H_{23},0.3575),(H_{23},0.8880),(H_{33},0.8880)\}$
4	$S_t(a_3^1, a_1^2, a_2^3, a_2^4)$	$\{(H_{11},0.3370),(H_{11},0.6630),(H_{11},0.8880),(H_{12},0.8880),(H_{11},0.3370),(H_{12},0.6630),(H_{12},0.8880),(H_{22},0.8880),(H_{22},0.3370),(H_{23},0.6630),(H_{23},0.8880),(H_{33},0.8880)\}$
5	$S_t(a_4^1, a_2^2, a_2^3, a_1^4)$	$\{(H_{12},0.3140),(H_{22},0.7430),(H_{22},0.6860),(H_{23},0.7430)\}$
6	$S_t(a_4^1, a_2^2, a_2^3, a_2^4)$	$\{(H_{33},0.9667),(H_{34},0.3140),(H_{34},0.9667),(H_{44},0.6860)\}$
7	$S_t(a_5^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{12},0.6804),(H_{22},0.7380),(H_{22},0.6804),(H_{23},0.7380),(H_{23},0.6804),(H_{33},0.7380)\}$
8	$S_t(a_5^1, a_1^2, a_2^3, a_1^4)$	$\{(H_{11},0.3610),(H_{11},0.4585),(H_{11},0.7380),(H_{11},0.7380),(H_{11},0.3610),(H_{11},0.4585),(H_{11},0.7380),(H_{12},0.7380),(H_{12},0.3610),(H_{22},0.4585),(H_{22},0.7380),(H_{23},0.7380)\}$
9	$S_t(a_5^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{12},0.5520),(H_{22},0.2620),(H_{22},0.7380),(H_{23},0.7380),(H_{22},0.5520),(H_{23},0.2620),(H_{23},0.7380),(H_{33},0.7380),(H_{23},0.5520),(H_{33},0.2620),(H_{33},0.7380),(H_{34},0.7380)\}$
10	$S_t(a_5^1, a_1^2, a_2^3, a_2^4)$	$\{(H_{11},0.2620),(H_{11},0.9100),(H_{11},0.7380),(H_{11},0.9100),(H_{11},0.2620),(H_{11},0.9100),(H_{11},0.7380),(H_{12},0.9100),(H_{12},0.2620),(H_{22},0.9100),(H_{22},0.7380),(H_{23},0.9100)\}$
11	$S_t(a_{11}^1, a_1^2, a_1^3, a_1^4)$	$\{(H_{11},0.6417),(H_{11},0.3740),(H_{11},0.6417),(H_{12},0.6260),(H_{12},0.6417),(H_{22},0.3740),(H_{22},0.6417),(H_{23},0.6260),(H_{22},0.6417),(H_{23},0.3740),(H_{23},0.6417),(H_{33},0.6260),(H_{23},0.6417),(H_{33},0.3740),(H_{33},0.6417),(H_{34},0.6260)\}$
12	$S_t(a_{11}^1, a_1^2, a_1^3, a_2^4)$	$\{(H_{12},0.5070),(H_{22},0.3740),(H_{22},0.6260),(H_{23},0.6260),(H_{22},0.5070),(H_{23},0.3740),(H_{23},0.6260),(H_{33},0.6260),(H_{23},0.5070),(H_{33},0.3740),(H_{33},0.6260),(H_{34},0.6260)\}$

Step 4: Aggregate the activated rules

The inference procedure is implemented by applying ULWA operator to combine the activated rules, $w_k^{\wedge}$ and $w_k^{\wedge}$ using Equations 5.20-5.21 for in this study. The final matching degree for activated rules of a scenario are calculated in the form of uncertain linguistic variables for identified scenarios and presented in Table 5.12.

Table 5.12 : Aggregation results of the activated rules.

No	Threat Scenario	$ULWA_{\wedge}$		$ULWA_{\vee}$	
		Uncertain Linguistic variable	Correspoding discrete terms	Uncertain Linguistic variable	Correspoding discrete terms
1	$(a_3^1, a_1^2, a_1^3, a_1^4)$	$[s_{2.2894}, s_{2.7714}]$	H_{23}	$[s_{2.3010}, s_{2.8238}]$	H_{23}
2	$(a_3^1, a_1^2, a_2^3, a_1^4)$	$[s_{1.9515}, s_{2.5907}]$	H_{13}	$[s_{1.9305}, s_{2.3196}]$	H_{13}
3	$(a_3^1, a_1^2, a_1^3, a_2^4)$	$[s_{2.0713}, s_{2.5713}]$	H_{23}	$[s_{2.0897}, s_{2.5897}]$	H_{23}
4	$(a_3^1, a_1^2, a_2^3, a_2^4)$	$[s_{1.5456}, s_{1.9864}]$	H_{12}	$[s_{1.5466}, s_{2.0257}]$	H_{13}
5	$(a_4^1, a_2^2, a_2^3, a_1^4)$	$[s_{1.7754}, s_{2.2754}]$	H_{13}	$[s_{1.8737}, s_{2.2989}]$	H_{13}
6	$(a_4^1, a_2^2, a_2^3, a_2^4)$	$[s_{3.0693}, s_{3.5693}]$	H_{34}	$[s_{3.2339}, s_{3.6705}]$	H_{34}
7	$(a_5^1, a_1^2, a_1^3, a_1^4)$	$[s_{2.0000}, s_{2.5000}]$	H_{23}	$[s_{2.0135}, s_{2.5068}]$	H_{23}
8	$(a_5^1, a_1^2, a_2^3, a_1^4)$	$[s_{1.2560}, s_{1.5090}]$	H_{12}	$[s_{1.2809}, s_{1.5477}]$	H_{12}
9	$(a_5^1, a_1^2, a_1^3, a_2^4)$	$[s_{2.2270}, s_{2.7270}]$	H_{23}	$[s_{2.2801}, s_{2.8012}]$	H_{23}
10	$(a_5^1, a_1^2, a_2^3, a_2^4)$	$[s_{1.2704}, s_{1.5533}]$	H_{12}	$[s_{1.3024}, s_{1.5485}]$	H_{12}
11	$(a_{11}^1, a_1^2, a_1^3, a_1^4)$	$[s_{1.7934}, s_{2.1945}]$	H_{13}	$[s_{1.9280}, s_{2.3854}]$	H_{13}
12	$(a_{11}^1, a_1^2, a_1^3, a_2^4)$	$[s_{2.2179}, s_{2.7179}]$	H_{23}	$[s_{2.2727}, s_{2.7831}]$	H_{23}

Step 5: Evaluate the security risks

At this step, the security risk of identified scenarios are ranked and compared based on their uncertain linguistic variables. The results are interpreted to guide SRA. The ranking of 12 identified threat scenarios based on their security risks is calculated and presented in Table 5.13. Rankings enable the DMs to identify the higher security risk scenarios from the lower security risk ones.

As seen from Table 5.12 and Table 5.13, after ranking, threat scenario 6 has the highest security risk with referential linguistic value, H_{34}, “Medium-High” and threat scenario 8 has the lowest security risk with referential linguistic value, H_{12}, “Very Low-Low” for both disjuntive and conjunctive rule antecedent aggregation. From the

results, it is observed that proposed model provides enough resolution for DMs to determine the security risk priorities of a critical facility. For example, although threat scenario 1, 3, 7, 9 and 12 have the same referential linguistic value, H_{23}, "Low-Medium", their security risks can be distinguished based on their uncertain linguistic variables. The arbitrary numeric scale problem is also solved since the security risk is modelled as uncertain linguistic variable. Lastly, problem of multiplicative aggregation that produces exactly the same value of security risk scores for different sets of T, V and C ratings with different security risk implications is solved. For example, scenario 7 is a High Likelihood-Low Consequence scenario and scenario 10 is a Low Likelihood-High Consequence scenario with the same vulnerability. But, scenario 7 and scenario 10 have different security risk interpretations. Therefore, the proposed model can also distinguish this kind of different security risk interpretations. When disjuntive and conjunctive rule antecedent aggregation operators are compared, the results are consistent.

Table 5.13 : Security risk rankings of threat scenarios.

No.	Threat Scenario	Ranking				
		Threat Likelihood	Vulnerability	Consequence	Security Risk	
					Conjunctive	Disconjuctive
1	$(a_3^1, a_1^2, a_1^3, a_1^4)$	3	8	10	2	2
2	$(a_3^1, a_1^2, a_2^3, a_1^4)$	7	8	3	6	8
3	$(a_3^1, a_1^2, a_1^3, a_2^4)$	6	8	7	5	5
4	$(a_3^1, a_1^2, a_2^3, a_2^4)$	11	8	2	10	10
5	$(a_4^1, a_2^2, a_2^3, a_1^4)$	8	14	5	8	9
6	$(a_4^1, a_2^2, a_2^3, a_2^4)$	9	14	**1**	**1**	**1**
7	$(a_5^1, a_1^2, a_1^3, a_1^4)$	**1**	12	**12**	7	6
8	$(a_5^1, a_1^2, a_2^3, a_1^4)$	10	12	6	**12**	**12**
9	$(a_5^1, a_1^2, a_1^3, a_2^4)$	2	12	9	3	3
10	$(a_5^1, a_1^2, a_2^3, a_2^4)$	**12**	12	4	11	11
11	$(a_{11}^1, a_1^2, a_1^3, a_1^4)$	5	15	11	9	7
12	$(a_{11}^1, a_1^2, a_1^3, a_2^4)$	4	15	8	4	4

5.5 Concluding Remarks of Chapter 5

After a structured set of scenarios, their likelihoods, vulnerabilities and consequences have been quantified with different modes of uncertainty from the corresponding models of proposed SRA framework, aggregating them properly for evaluating the

security risk is needed. Therefore, the main goal of this chapter is to evaluate the security risk of a critical facility by aggregating security risk factors correctly. For this purpose, a new rule based expert system is proposed.

Firstly, problems about aggregation of security risk factors are addressed. It is stated that Security risk factors must be aggregated in a nonlinear rather than linear manner but multiplicative aggregation is not the right aggregation operator because of the inability to distinguish between High likelihood-low consequence and low likelihood-high consequence threat scenarios, unsuitable nonlinear manner, and arbitrary numeric scale problem. Then, handling various types of uncertain input information is investigated.

Secondly, a new rule-based system is designed and implemented for evaluating security risk. Transformations of input variables are done depending on the uncertainty mode of input variables by either fuzzification or bet estimate. A rule-base is designed with the rules having uncertain linguistic variable consequents for the reason of eliminating the arbitrary numeric scales problem. Since the outputs of activated rules are linguistic variables, ULWA operator is used for inference process. Therefore, proposed rule based expert system has different input variable transformation, different rule consequent and different rule aggregation method for inference process. For rule antecedent evaluation, two main aggregation strategies, both conjunctive and disconjunctive, are also applied and compared for the sensitivity analysis.

To summarize, proposed method offers a rational, reliable way to aggregate model outputs. By this way different formats of available data and uncertain knowledge can be incorporated into SRA process. Such a rule base is capable of capturing vagueness, incompleteness, and nonlinear causal relationships by representing them with if–then rules. This approach can capture nonlinear casual relationships as well as different kinds of uncertainty.

As a result, the proposed model is applied to a case study. Proposed methodology provides a flexible and effective inference procedure to deal with such multi uncertain information. It is capable of aggregating various types of uncertainties. According to the results of REM, suggestions for a critical facility protection can be put forward to reduce the security risks. REM enables security analyzers to identify

the higher security risk scenarios from the lower security risk ones. The proposed rule based expert system is generic rule-base inference methodology and can easily be applied to other applications that have arbitrary numeric scales problem and nonlinear casual relationships.

6. CONCLUSION AND RECOMMENDATIONS

SRA is a major component of modern security risk management and better risk management decisions are dependent on a better understanding of the concerned risk type. Correct SRA is crucial because defence resources are limited and there are not enough resources to eliminate all security risks of a critical facility. Realistic SRA is required to support strategies for identifying, controlling, reducing, and finally managing security risks. Without clear SRA, DMs cannot also benchmark improvements or progress to reduce the overall risk level.

In this thesis, after the potential limitations of conventional RA methods are identified, the required theories, methodologies and information about SRA are explored and researched. Since the main goal of this thesis is to accomplish correct SRA by more realistically quantifying security risk factors and alleviating the previously mentioned concerns to some degree, systematic and rigorous SRA framework that provides adequate information to guide security risk management process is proposed. Since there are many challenges in the details of SRA, the main research questions addressed in this thesis are as follows:

- How to measure/quantify/represent security risk factors: Threat likelihood, Vulnerability, Consequence, and Security risk considering appropriate uncertainty models?
- How to aggregate threat likelihood, vulnerability and consequence for SRA?
- How to improve SRA decisions?

The proposed SRA framework focuses on quantification of the three fundamental factors used to assess the security risk: threat, vulnerability and consequence and aggregation of them for SRA. In order to accomplish SRA, four different models are developed for each factor of the SRA framework as Threat Assessment Model (TAM), Vulnerability Assessment Model (VAM), Consequence Assessment Model (CAM), and Risk Evaluation Model (REM). Each developed model in SRA framework proposes an approach for quantification of corresponding security risk

factor. Therefore, proposed SRA framework has been studied in three dimensions: theoretical framework, methodological framework and information processing framework and described in detail.

The first model of the proposed SRA framework, TAM, identifies threats of a critical facility and estimates their likelihoods (Chapter 2). For this purpose, a novel approach called evidence based Morphological Analysis (EMA) model is proposed based on Dempster-Shafer theory of evidence (DST) and Morphological Analysis (MA) methodology by describing reasons for modelling uncertainty by DST, the fundamentals of DST and MA, and how DST is applied for threat likelihood estimation within MA. The proposed approach is presented step by step and applied to a simple case study on airport threat assessment. The results show that EMA can be used to reason about threat assessment by providing adequate precision and better captures the uncertainty in threat assessment than traditional probabilistic risk approaches that use point estimates. TAM also generates the initiating events, possible threat scenarios, for the other models of SRA framework.

The second model of the proposed SRA framework, VAM, identifies and quantifies the weakness of the critical facility as a system, system functions and system components, and determines the most critical functions and components by simulating the system behaviour (Chapter 3). For this purpose, a new approach called fuzzy integrated vulnerability assessment model (FIVAM) based on fuzzy set theory, Simple Multi-Attribute Rating Technique (SMART) and Fuzzy Cognitive Maps (FCM) methodology in a group decision-making environment is proposed. The FIVAM approach is presented step by step and applied to a simple case study on airport vulnerability assessment. The results of the application are compared to those observed through a classical vulnerability assessment model to illustrate the effectiveness of the FIVAM. The results show that FIVAM provides both a framework to identify the hidden vulnerabilities caused by the functional interdependencies within the system and a relative ranking of targets that might require improved protection.

The third model of the proposed SRA framework, CAM, estimates the expected magnitudes and types of losses (e.g., deaths, injuries, or property damage) associated with a threat scenario given adversary success by identifying, quantifying and integrating all different types of losses specific to security risk of a critical facility

while estimating the total consequence (Chapter 4). For this purpose, Monte Carlo Simulation based CA model that combines different types of consequences for SRA is proposed. The proposed approach is presented step by step and applied to a simple case study on airport consequence assessment. The results show that proposed model can be used to reason about consequence assessment by enabling security analyzers to identify the higher consequence scenarios from the lower consequence ones. The proposed model also performs CA by considering all major losses of security risk with optimal complexity and time to improve the SRA.

The last model of the proposed SRA framework, REM, is an inference model that aggregates the outputs of TAM, VAM and CAM for evaluating the security risk of a critical facility (Chapter 5). For this purpose, new rule-based expert system is proposed for capturing nonlinear causal relationships between security risk factors (threat likelihood, vulnerability and consequence) which have different uncertainty modes for evaluating security risks. The proposed approach is presented step by step and applied to a simple case study on airport security risk evaluation. The results show that proposed model can be used to reason about security risk evaluation by enabling security analyzers to identify the higher security risk scenarios from the lower security risk ones and can capture nonlinear casual relationships as well as different kinds of uncertainty.

To summarize, proposed SRA framework is a multi methodological approach because methodologies relevant to address the special challenges of security risk factors are investigated and applied in a logical and efficient way. These include problem structuring methods (PSM) such as MA, multiple criteria/attribute decision making (MCDM) techniques such as SMART, data integration methods and evidence combination techniques such as rule based expert systems, DST combination rules and ULWA, and modelling and simulation techniques such as TNT equivalent method, FCM and Monte Carlo simulation. Secondly, since there are different sources/causes of uncertainty affecting security risk factors in SRA, different from conventional RA approaches proposed SRA framework represents each security factor with different uncertainty theory. Parameters of VAM are represented by belief functions of Dempster-Shafer (imprecision due to lack of knowledge/partial ignorance), parameters of CAM are represented by fuzzy membership functions (imprecision due to vagueness) and parameters of CAM are

represented by probability distributions (randomness due to variability). Therefore, proposed SRA framework handles various types of uncertainties as randomness, incompleteness and fuzziness. Thirdly, different uncertainty theories are combined effectively by the proposed SRA framework providing solutions for nonlinear aggregation problem as in multiplicative aggregation and arbitrary numeric scale problem. So, this thesis proposes a complete SRA framework that offers a comprehensive and logical multi methodological approach capable of handling and combining different uncertainties as partial ignorance, fuzziness and randomness for assessing the security risk of critical facilities.

After SRA has been completed by applying proposed SRA framework, its results can be used to improve security risk management decision making by allocating available risk management resources to security risk-reducing countermeasures (e.g., for vulnerability reduction increasing surveillance and detection, hardening targets etc. or for consequence reduction increasing preparedness and response). SRA help to formulate the requirements for protection measures necessary to counter the perceived threat.

Security risk is dynamic because security managers as defenders are constantly making investments to reduce threat, vulnerability and consequence, and adversaries as attackers constantly alter preferences of targets and capabilities. Since SRA is a continuous process, the new information obtained can be easily can be used easily as a feedback for the proposed framework to update security risk evaluation. As some standard for estimating and monitoring change is needed, proposed framework can also be used for security risk monitoring. In addition to this, the proposed SRA framework is generic enough to be applied to any type of critical facility with minor modifications such as dam, governmental facility, harbour, nuclear power plant, oil plant etc. by insurance companies, municipal managers, etc.

As a result, proposed SRA framework has contributed to quantitative decision analysis by supporting decisions under different modes of uncertainty and provided a basis for more effective security risk management. Proposed framework also provides easy security risk communication and the dissemination of security risk information in an understandable form. The proposed framework is very useful for the systematic and rational SRA. Its feasibility and effectiveness are illustrated by numerical examples in each chapter. It is seen that useful insight about possible

security risks of a critical facility can be gained through applying proposed SRA framework and proposed framework provides valuable information to DMs in dealing with security risks of critical facility by increasing situational awareness and understanding.

REFERENCES

Akgün İ., Kandakoğlu A. and Özok A. F. 2010. Fuzzy Integrated Vulnerability Assessment Model for Critical Facilities in Combating the Terrorism, *Expert Systems with Applications*, **37**, 3561-3573.

Andrews, J. D. and Dunnett, S. J. 2000. Event Tree Analysis using Binary Decision Diagrams, *IEEE Trans. Reliability*, **49**, June, 230-238.

Apostolakis G. E and Lemon D. M. 2005. A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism, *Risk Analysis*, **25**, 361-376.

Apostolakis, G. E., 2004. How useful is Quantitative Risk Assessment?, *Risk Analysis*, **24** (3), 1-6.

Arunraj, N.S. and Maiti, J. 2009. A methodology for overall consequence modelling in chemical industry, *Journal of Hazardous Materials*, **169**, 556-574.

Ashford N., Stanton H. P. M., Moore C. A. 1997. *Airport Operations, 2nd edition*. McGraw-Hill, London.

Axelrod, R. 1976. *Structure of Decision: The Cognitive Maps of Political Elites*. Princeton University Press, Princeton NJ.

Bajpai, S. and Gupta, J. P. 2005. Site security for chemical process industries, *Journal of Loss Prevention in the Process Industries*, **18**, 301-309.

Bajpai, S. and Gupta, J. P. 2007. Securing oil and gas infrastructure, *Journal of Petroleum Science and Engineering*, **55**, 174-186.

Brown, T., Beyeler, W., Barton, D. 2004. Assessing infrastructure interdependencies: The challenge of risk analysis for complex adaptive systems, *International Journal of Critical Infrastructures*, **1**(1), 108-117.

Brownlow, S. A. and Watson, S. R. 1997. Structuring multiattribute value hierarchies, *Journal of Operational Research Society*, **38**, 309-318.

Chen, S. J. and Hwang, C. L. 1992. *Fuzzy multiple attribute decision-making method and applications.* Springer-Verlag, Berlin.

Chou, S. Y. and Chang, Y. H. 2008. A decision support system for supplier selection based on a strategy-aligned fuzzy SMART approach, *Expert Systems with Applications*, **34**, 2241–2253.

Cooper P. W., 1996. *Explosive Engineering*, Wiley-VCH, Germany.

Cox L.A., Babayev D. and Huber W., 2005. Some limitations of qualitative risk rating systems, *Risk Analysis*, **25** (3), 651-662.

Demotier, S., Schön, W. and Denoeux T. 2006. Risk Assessment Based on Weak Information Using Belief Functions: A Case Study in Water Treatment, *IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and Reviews*, **36** (3), 382-396.

Dempster, A. P. 1967. Upper and Lower Probabilities Induced by a Multivalued Mapping, *The Annals of Statistics*, **28**, 325-339.

Dempster, A. P., Yager, R. R. and Liu L. 2008. *The Classic Works on the Dempster-Shafer Theory of Belief Functions*, Springer-Verlag, Berlin.

Diaz Alonso F., Gonzalez Ferradas E., Doval Minarro M., Minana Aznar A., Ruiz Gimeno J. and Sanchez Perez J. F., 2008. Consequence analysis by means of characteristic curves to determine the damage to buildings from the detonation of explosive substances as a function of TNT equivalence, *Journal of Loss Prevention in the Process Industries*, **21** (1), 74-81.

Diaz Alonso F., Gonzalez Ferradas E., Sanchez Perez J. F., Minana Aznar A., Ruiz Gimeno J. and Martinez Alonso J., 2007. Consequence analysis by means of characteristic curves to determine the damage to humans from the detonation of explosive substances as a function of TNT equivalence, *Journal of Loss Prevention in the Process Industries*, **20** (3), 187-193.

Diaz Alonso F., Gonzalez Ferradas E., Sanchez Perez J. F., Minana Aznar A., Ruiz Gimeno J. ve Martinez Alonso J., 2006. Characteristic overpressure–impulse–distance curves for the detonation of explosives, pyrotechnics or unstable substances, *Journal of Loss Prevention in the Process Industries*, **19** (6), 724-728.

Dickerson, J. A. and Kosko, B. 1997. Virtual worlds as fuzzy cognitive maps, in *Fuzzy engineering*, p.125-141, Ed. Kosko, B. Prentice-Hall, Upper Saddle River.

Dubois, D. and Prade, H., 1988. *Possibility Theory*, Plenum Press, New York.

Dubois, D. and Prade, H., 1992. On the combination of evidence in various mathematical frameworks. In J. Flamm and T. Luisi (eds) *Reliability Data Collection and Analysis*, Springer, Berlin. pp. 213-241.

Edwards, W. 1971. *Social Utilities, Engineering Economist*, Summer Symposium Series 6, 119-129.

Edwards, W. 1977. How to use multiattribute utility measurement for social decision making, *IEEE Transactions on Systems, Man and Cybernetics*, **7**, 326-340.

Edwards, W. and Barron, F. H. 1994. SMARTS and SMARTER: Improved simple methods for multi attribute utility measurement, *Organizational Behaviour and Human Decision Processes*, **60**, 306-325.

Ericson C., 1999. Fault tree analysis: A history, *Proceedings of the 17th International System Safety Conference*. August, 1999. Orlando Florida.

Ezell B. C., Bennett S.P., Winterfeldt D., Sokolowski J. and Collins A.J. 2010. Probabilistic Risk Analysis and Terrorism Risk, *Risk Analysis*, **30** (4), 575-589.

Ezell B., Haimes Y., and Lambert J. 2001. Risk of cyber attack to water utility supervisory control and data acquisition systems, *Military Operations Research*, **6**(2), 30-46.

Ezell, B. C. 2007. Infrastructure Vulnerability Assessment Model (I-VAM), *Risk Analysis*, **27** (3), 571-583.

Garrick B. J., Hall, J.E., Kilger, M., McDonald, J.C., O'Toole, T., Probst, P.S., Rindskopf Parker, E., Rosenthal, R., Trivelpiece, A.W., van Arsdale, L.A., Zebroski, E.L. 2004. Confronting the risks of terrorism: making the right decisions. *Reliability Engineering & System Safety*, **86** (2), 129-176.

Guyonnet D., Bourgine B., Dubois D., Fargier H., Come B., and Chiles J.P. 2003. Hybrid Approach for Addressing Uncertainty in Risk Assessments. *Journal of Environmental Engineering*, 129 (1), 68-79.

Harris, B. 2004. Mathematical methods in combating terrorism, *Risk Analysis*, **24**(4) 985–988.

Helton J. C., 1997. Uncertainty and Sensitivity Analysis in the Presence of Stochastic and Subjective Uncertainty, *Journal of Statistical Computation and Simulation*, **57**, 3-76.

Huang, B. and Cheng, F., 2009. Consequence Simulation of Vapour Cloud Explosion in *LPG Storage Tank, Advances in Intelligent System Research Vol 9*, New Perspectives on Risk Analysis and Crisis Response, 19-21 October 2009. Beijing, China, pp. 319-325.

Jackson, P. 1998. *Introduction To Expert Systems (3 ed.)*, Addison Wesley, ISBN 978-0-201-87686-4

Jang J.-S.R., Sun C.-T., Mizutani E., 1997. *Neuro-Fuzzy and Soft Computing: A Computational Approach to Learning and Machine Intelligence*, First Edition, Prentice Hall, New Jersey.

Kaplan S. and Garrick B.J., 1981. On the quantitative definition risk, *Risk Analysis*, **1**, 11-27.

Kaufmann, A. and Gupta, M. M. 1991. *Introduction to Fuzzy Arithmetic-Theory and Applications*, Van Nostrand Reinhold, New York.

Keeney R. L., 2007. Modeling Values for Anti-Terrorism Analysis, *Risk Analysis*, **27** (3), 585-596.

Khan, F.I., and Abbasi, S.A., 1998. Rapid quantitative risk assessment of a petrochemical industry using a new software MAXCRED, *Journal of Cleaner Production*, **6**, 9–22.

Khan, F.I., and Abbasi, S.A., 1999. HAZDIG: a new software package for assessing the risks of accidental release of toxic chemicals, *Journal of Loss Prevention in the Process Industries*, **12**, 167–181.

Khan, F.I., and Abbasi, S.A., 2000. TORAP—a new tool for conducting rapid risk-assessments in petroleum refineries and petrochemical industries, *Applied Energy*, **65** (1–4), 187–210.

Khan, F.I., and Haddara, M. 2004. Risk-based maintenance (RBM): a new approach for process plant inspection and maintenance, *Process Safety Progress*, **23** (4), 252–265.

Kirchsteiger C., 1999. On the use of probabilistic and deterministic methods in risk analysis, *Journal of Loss Prevention in the Process Industries*, **12**, 399-419.

Knuth, D., 1997. *The Art of Computer Programming, Volume 3: Sorting and Searching, Third Edition*. Addison-Wesley, Boston.

Kolmogorov A. N., 1950. *Foundations of the Theory of Probability*. Chelsea Pub. Co., UK.

Kosko, B. 1986. Fuzzy cognitive maps, *International Journal on Man–Machine Studies*, **24** (1), 65-75.

Kosko, B. 1991. *Neural networks and fuzzy systems*, Prentice-Hall, Englewood Cliffs.

Laplace P. S. 1812. *Analytical Theory of Probability*. Courier. Paris.

LaTourrette T., Howell D.R.,Mosher D.E., and MacDonald J., 2006. *Reducing Terrorism Risk at Shopping Centers: An Analysis of Potential Security Options*, RAND Corporation, Santa Monica, CA.

Lee, C. 1990. Fuzzy logic in control systems: Fuzzy logic controller, Part I and II. *IEEE Transactions on Systems, Man and Cybernetics*, **20**, 404-435.

Levitin G., Ben-Haim H., 2008. Importance of protections against intentional attacks, *Reliability Engineering and System Safety*, **93**, 639–646.

Liang, G. S. 1999. Fuzzy MCDM based on ideal and anti-ideal concepts, *European Journal of Operational Research*, **112**, 682–691.

Liu C, Grenier D., Jousselme A., Bosse E, 2007. Reducing Algorithm Complexity for Computing an Aggregate Uncertainty Measure, *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, **37** (5), 669-679.

Mamdani, E.H. and S. Assilian, 1975. An experiment in linguistic synthesis with a fuzzy logic controller, *International Journal of Man-Machine Studies*, **7** (1), 1-13.

McGill W. L., Ayyub B. M., and Kaminskiy M., 2007. Risk Analysis for Critical Asset Protection, *Risk Analysis*, **27** (5), 1265-1281.

Merigo J.M. and Casanovas M., 2010. Linguistic aggregation operators for linguistic decision making based on the Dempster-Shafer theory of evidence, International *Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, **18** (3), 287-304.

Min, H. J., Beyeler, W., Brown, T., Son, Y. J. and Jones, A. T. 2007. Toward modeling and simulation of critical national infrastructure interdependencies, *IIE Transactions*, **39**, 57–71.

Murray, A. T., Matisziw, T. C., Grubesic, T. H. 2007. Critical network infrastructure analysis: interdiction and system flow, *Journal of Geographical Systems*, **9**, 103–117.

Oberkampf W.L., Helton J.C., Joslyn C.A., Wojtkiewicz S.F., Ferson S., 2004. Challenge problems: uncertainty in system response given uncertain parameters, *Reliability Engineering & System Safety*, **85**, 11-19.

Remennikov, A.M., 2003. A Review of Methods for Predicting Bomb Blast Effects on Buildings, *Journal of Battlefield Technology*, **6**(3) 5-10.

Renn, O. 1992. Concepts of risk: A classification, in *Social Theories of Risk*, Eds., Krimsky, S. and Golding, D., Praeger, Westport CT.

Ritchey, T., 1998. General morphological analysis: a general method for non-quantified modelling, http://www.swemorph.com/pdf/gma.pdf Accessed at 12.01.2010.

Ritchey, T., 2009. Futures studies using morphological analysis, http://www.swemorph.com/pdf/futures.pdf, Accessed at 12.01.2010.

Rosoff H., and von Winterfeldt D., 2007. A risk and economic analysis of dirty bomb attacks on the ports of Los Angeles and Long Beach, *Risk Analysis*, **27**(3), 533-546.

Ross, T. J. 1995. *Fuzzy Logic with Engineering Applications*, McGraw-Hill, New York.

Rubinstein, R.Y., and Kroese, D.P. 2007. *Simulation and the Monte Carlo Method*, 2nd edition, John Wiley and Sons, New York.

Salmeron, J., Wood, K., Baldick, R. 2004. Analysis of electric grid security under terrorist threat, *IEEE Trans. Power Systems*, **19**(2), 905-912.

Sarewitz, D., Pielke, R. Jr., and Keykhah, M. 2003. Vulnerability and Risk: Some Thoughts from a Political and Policy Perspective, *Risk Analysis*, **23** (4), 805-810.

Sentz, K. and Ferson, S., 2002. *Combination of Evidence in Dempster-Shafer Theory*, Sandia National Laboratories Report, SAND2002-0835.

Shafer G., 1976. *A mathematical theory of evidence*, Princeton University Press, Princeton.

Sharif A. M. and Irani Z., 2006a. Applying a fuzzy-morphological approach to complexity management decision making, *Management Decision*, **44**(7), 930-961.

Sharif, A. M. and Irani, Z. 2006b. Exploring fuzzy cognitive mapping for IS evaluation, *European Journal of Operational Research*, **173**, 1175–1187.

Simpson J. and Weiner E., 1989. *The Oxford English Dictionary*, Second Edition, Clarendon Press, UK.

Smets P., 2000. Data Fusion in the transferable Belief Model, *Proceedings of 3rd International Conference on Information Fusion*, Fusion 2000, Paris, France, pp. 21-33, July, 2000.

Smets P., 2007. Analyzing the combination of conflicting belief functions, *Information Fusion*, 8, 387-412.

Stach, W., Kurgan, L., Pedrycz, W., Reformat, P. 2005. Genetic learning of fuzzy cognitive maps, *Fuzzy Sets and Systems*, **153**, 371–401.

State Airport Authority (SAA) 2009. *Yıllık İstatistiki Uçak ve Yolcu Verileri*, http://www.dhmi.gov.tr, accessed at

Sugeno, M. 1985. An introductory survey of fuzzy control, *Information Sciences*, **36**, 59-83.

Turkish Statistical Office (Turkstat) 2009. *Bölgesel İstatistikler: 2001 Yılı Cari Fiyatlarına Göre Kişi Başına Düşen GSYH*, http://tuikapp.tuik.gov.tr, accessed at

Usmani Z. and Kirk D., 2008. Emergency 101- Suicide Bombers, Crowd formations and blast waves, *Proceedings of IEEE, Military Communication Conference*, 16-19 November, 2008. San Diego, CA, pp. 1-7.

Usmani Z., Alghamdi F.A. and Kirk D., 2009. BlastSim-Multi Agent Simulation of Suicide Bombing, *Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defence Applications* (CISDA 2009), Ottawa, ON, pp.1-8.

Wang, Y. M., Yang, J. B., and Xu, D. L. 2005. A preference aggregation method through the estimation of utility intervals, *Computers & Operations Research*, **32** (8), 2027-2049.

Wang, Y. M., Yang, J. B., and Xu, D. L. 2006. Environmental impact assessment using the evidential reasoning approach. *European Journal of Operational Research*, **174** (3), 1885–1913.

Willis H.H., Morral A.R., Kelly T.K., and Medby J., 2005. *Estimating Terrorism Risk*, MG-388-RC. RAND Corporation, Santa Monica, CA.

Willis, H. H. 2007. Guiding Resource Allocation Based on Terrorism Risk, *Risk Analysis*, **27**(3), 597-606.

Wright D., Liberatore M. J., Nydick R. L., 2006. A Survey of Operations Research Models and Applications in Homeland Security, *Interfaces*, **36** (6), 514-529.

Xirogiannis, G., Stefanou, J. and Glykas, M. 2004. A fuzzy cognitive map approach to support urban design, *Expert Systems with Applications*, **26**, 257-268.

Xu Z. 2004. Uncertain linguistic aggregation operators based approach to multiple attribute group decision making under uncertain linguistic environment, *Information sciences*, **168**, 171-184.

Yager, R. 1987a. On the Dempster-Shafer Framework and New Combination Rules. *Information Sciences*, **41**, 93-137.

Yager, R. 1987b. Quasi-Associative Operations in the Combination of Evidence. *Kybernetes*, **16**, 37-41.

Yang, J.B., and Singh, M.G., 1994. An evidential reasoning approach for multiple attribute decision making with uncertainty. *IEEE Transactions on Systems, Man, and Cybernetics*, **24** (1), 1–18.

Yetton, P., and Bottger, P. 1983. The relationships among group size, member ability, social decision schemes, and performance. *Organizational Behavior and Human Performance*, **32** (2), 145–159.

Yoon, K. P. and Hwang, C. L. 1995. *Multiple Attribute Decision Making: An Introduction, Sage Publications*, Thousand Oaks, CA.

Zadeh L. 1965. Fuzzy Sets, *Information and Control*, **8**, 338-358.

Zadeh L. 1978. Fuzzy Sets as a Basis for a Theory of Possibility, *Fuzzy Sets and Systems*, **1**(1), 3-28.

Zadeh, L.A. 1975a. The concept of a linguistic variable and its application to approximate reasoning-I. *Information Sciences*, **8** (3), 199-249.

Zadeh, L.A. 1975b. The concept of a linguistic variable and its application to approximate reasoning-II. *Information Sciences*, **8** (4), 301-357.

Zadeh, L.A. 1975c. The concept of a linguistic variable and its application to approximate reasoning-III. *Information Sciences*, **9** (1), 43-80.

Zimmermann H. J., 2000. An application-oriented view of modeling uncertainty, *European Journal of Operational Research*, **122**, 190-198.

Zwicky, F. 1969. *Discovery, Invention, Research – Through the Morphological Approach*, The MacMillian Company, Toronto.

CURRICULUM VITAE

Candidate's full name: İlker AKGÜN

Place and date of birth: İzmit/KOCAELİ, 1975

Permanent Address: İstanbul

Universities and Colleges attended:

M.Sc.: Istanbul Technical University Istanbul, TURKEY, Computer Engineering, 2000-2004

Middle East Technical University Ankara, TURKEY, Modelling and Simulation, 2000-2002

Diploma: Bogazici University, Istanbul, TURKEY, Computer Engineering, 1998-1999

B.A.: Naval Academy Istanbul, TURKEY, Computer and Control Systems Engineering, 1993-1997

High School: Naval High School, Heybeliada/Istanbul, TURKEY, 1990-1993

Publications:

▪ **Akgün İ.,** Kandakoğlu A. and Özok A.F., 2010. Fuzzy Integrated Vulnerability Assessment Model for Critical Facilities in Combating the Terrorism, *Expert Systems with Applications*, **37**, 3561-3573.

▪ Çukurtepe H., **Akgün İ.,** 2009. Towards Space Traffic Management System, *Acta Astronautica*, **65**(5-6), 870-878.

▪ Kandakoğlu A., Çelik M., **Akgün İ.,** 2009. A Multi-Methodological Approach for Shipping Registry Selection in Maritime Transportation Industry, *Mathematical and Computer Modelling*, **49** (3-4), 586-597.

▪ **Akgün İ.,** Buzluca F., 2006. Virtual topology reconfiguration on optical WDM networks considering traffic grooming, *Optical Switching and Networking*, **3** (1), 11-23.